EXECUTIVE SERIES

TREND MICRO™

Espionage as a Service

Cybercrime-as-a-Service Series

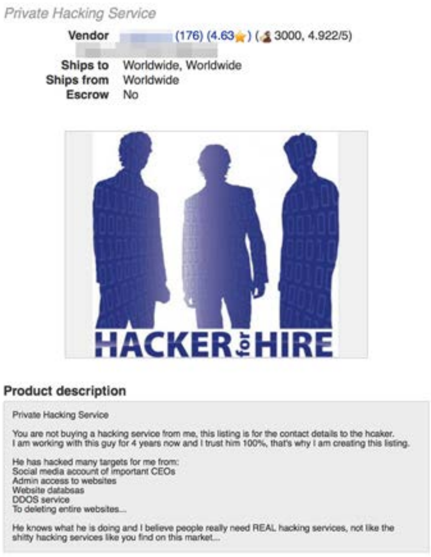
Cybercrime as a service (CaaS) is an important trend in Deep Web forums because it puts cybercriminal tools and services in the hands of a wider range of threat actors—even the nontechnical, such that anyone can become a cybercriminal with minimal investment. At the same time, cybercriminals are now seeing the advantages of expanding their targets from home users to larger enterprise networks. This is a matter that enterprises need to be ready for.

How Espionage as a Service Works

Many discussions on espionage focus on how nation-states steal another's intellectual property, top-secret plans, and other high-value information via cyber attacks. Enterprises, however, are not exempt from spying. Compared with other much-discussed threats to confidential corporate data or "company crown jewels" such as ransomware and distributed denial-of-service (DDoS) attacks, very few are aware of espionage-as-a-service (EsaaS) offerings in underground markets and the Deep Web[1] that can impact victims' bottom line.

The United States, for instance, spends more on research and development (R&D) than any other country worldwide. Developing unique offerings to gain a competitive edge requires a lot of effort and resources. Economic espionage can cost the United States alone billions of dollars each year. While it is not new, it is growing, and theft attempts by competitors and adversaries are becoming more brazen and varied.[2]

Attackers can easily obtain espionage tools and services underground to spy on and steal company crown jewels that they can then sell to the victims' highest-bidding competitors or use to further line their pockets via extortion. Bidders could be seeking competitive or strategic advantages over rivals or disgruntled former employees who wish to take previous employers down.



Private Hacking Service

Vendor [redacted] (176) (4.63★) (3000, 4.922/5)

Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow No

Product description

Private Hacking Service

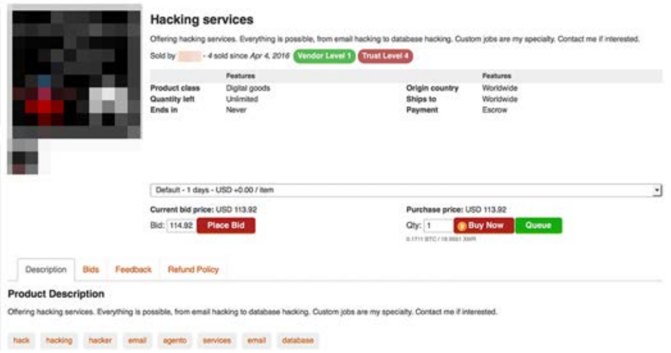
You are not buying a hacking service from me, this listing is for the contact details to the hcaker.
I am working with this guy for 4 years now and I trust him 100%, that's why I am creating this listing.

He has hacked many targets for me from:
Social media account of important CEOs
Admin access to websites
Website databsas
DDOS service
To deleting entire websites...

He knows what he is doing and I believe people really need REAL hacking services, not like the shitty hacking services like you find on this market...

Figure 1: Deep Web ad for corporate-account-hacking services; prices depend on the job's complexity

Some espionage-as-a-service offerings available underground include database-, Web-server-, website-, and email-hacking services; doxing (gathering data otherwise not publicly available on a chosen individual or company) services; and hacking tutorials and spying tools.



Hacking services

Offering hacking services. Everything is possible, from email hacking to database hacking. Custom jobs are my specialty. Contact me if interested.

Sold by [redacted] - 4 sold since Apr 4, 2016 Vendor Level 1 Trust Level 4

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

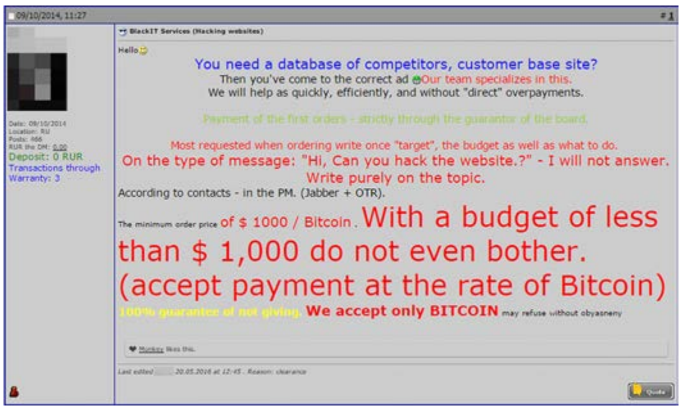
Current bid price: USD 113.92
Bid: 114.92 Place Bid

Purchase price: USD 113.92
Qty: 1 Buy Now Queue
0.1711 BTC / 16.8881 XMR

Product Description

Offering hacking services. Everything is possible, from email hacking to database hacking. Custom jobs are my specialty. Contact me if interested.

Figure 2: Deep Web ad for custom hacking services; prices vary, depending on the job's complexity



09/10/2014, 11:27 #1

Date: 09/10/2014
Location: RU
Posts: 466
RUR the DM: 0.00
Deposit: 0 RUR
Transactions through Warranty: 3

BlackIT Services (Hacking websites)

Hello

You need a database of competitors, customer base site?
Then you've come to the correct ad Our team specializes in this.
We will help as quickly, efficiently, and without "direct" overpayments.

Payment of the first orders - strictly through the guarantor of the board.

Most requested when ordering write once "target", the budget as well as what to do.
On the type of message: "Hi, Can you hack the website.?" - I will not answer.
Write purely on the topic.
According to contacts - in the PM. (Jabber + OTR).

The minimum order price of $ 1000 / Bitcoin. With a budget of less than $ 1,000 do not even bother. (accept payment at the rate of Bitcoin)
100% guarantee of not giving. We accept only BITCOIN may refuse without obyasneny

Munkey likes this.

Last edited [redacted] 20.05.2016 at 12:45 . Reason: clearance

Figure 3: Russian underground forum ad for hacking a business rival's database

The huge amounts of money that individuals and companies shell out to get their hands on rivals' crown jewels entices an increasing number of cybercriminals to peddle espionage-as-a-service offerings. The fact that hackers are very hard to track and apprehend, and that related tools and services are easy to provide and procure, is contributing to the proliferation of espionage as a service. Law enforcement agencies would much rather focus on capturing nation-state actors as well, further decreasing risks to cybercriminals engaging in the business.

What This Means for Enterprises

We have seen governments and public agencies succumb to nation-state espionage attacks. Enterprises have to keep in mind, however, that all companies, regardless of industry and size, can fall prey to espionage attacks.

Companies in the United States can, according to a 2015 ITProPortal study,[3] lose a whopping US$300 billion to intellectual property theft each year. In the United Kingdom, meanwhile, a 2011 Detica report[4] pegged the total cost of cybercrime at £27 billion each year. Some £9.2 billion of the said amount could be attributed to intellectual property theft while £7 billion accounted for losses due to corporate espionage.

> The total cost of cybercrime (data theft) worldwide is expected to reach US$2 trillion by 2019.[5]

Corporate espionage can cause a company to lose highly confidential assets such as blueprints, patents, product designs, works in progress (technologies, products, or services in development), unique processes, and mergers and acquisitions (M&A) data, among others that can affect its bottom line. Other effects include:

- Loss of competitive edge over business rivals
- Brand and reputation damage
- Loss of potential profits from technologies, products, or services in the works
- Dwindling financial resources due to the payment of huge attack-recovery costs

There exists a very thin line between targeted[6] and EsaaS attacks; the latter just has an extra step. They essentially employ the same tools, tactics, and techniques. The EsaaS attack chain comprises the following components:[7]

- **Conduct reconnaissance:** Attackers gather intelligence on intended targets. They look at targets' network infrastructure and company structure to identify who in the organization to go after in order to get the data they want to steal. At this stage, targets' crown jewels are identified.
- **Identify entry point:** Using the intel, attackers send a contextually relevant malware-laden spear-phishing email to bait the target. Social engineering ploys play a crucial role in how successful a spear-phishing campaign is. Attackers usually target high-ranking corporate officials in a technique called "whaling," as obtaining their credentials can open more doors than going after typical employees.
- **Infiltrate network:** Attackers establish command and control (C&C) over target networks aided by malware such as backdoors, remote access Trojans (RATs), and, at times, even Trojan spyware.

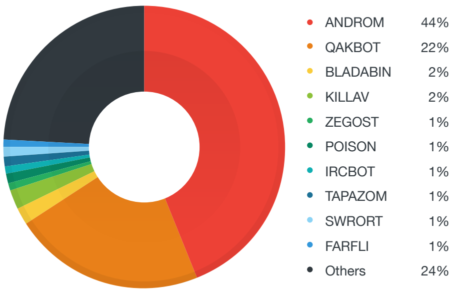


Figure 4: Most of today's top backdoors are old-but-reliable threats that can steal financial credentials, system and network details, server information, and all kinds of data (usernames and passwords) saved in cookies and browsers.

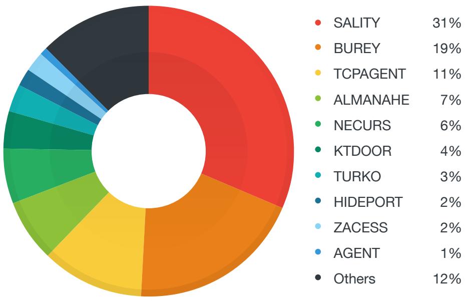


Figure 5: Rootkits hide traces of ongoing attacks by shielding malicious routines from detection or even shutting down anti-malware protection.

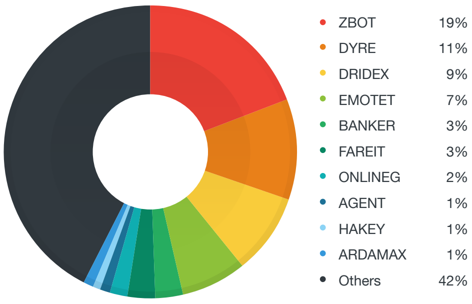


Figure 6: Run-of-the-mill Trojan spyware steal different kinds of information, most notably access credentials.

- **Achieve lateral movement:** Once attackers gain a foothold in target networks, they need to remain persistent while moving laterally until they infiltrate systems where the company crown jewels are actually stored.
- **Exfiltrate stolen data:** Once the company crown jewels are located, attackers need to exfiltrate or transfer stolen data without triggering security alarms to locations only they can access.
- **Sell stolen data to the highest bidders (usually business rivals) or extort money from victims:** This is an additional component for EsaaS attacks. Targeted attacks typically stop with data exfiltration, but because EsaaS attacks are considered a form of cybercrime, the last step always involves profits. Buyers of the stolen data may, of course, be pre-identified, as is the case with hackers for hire.

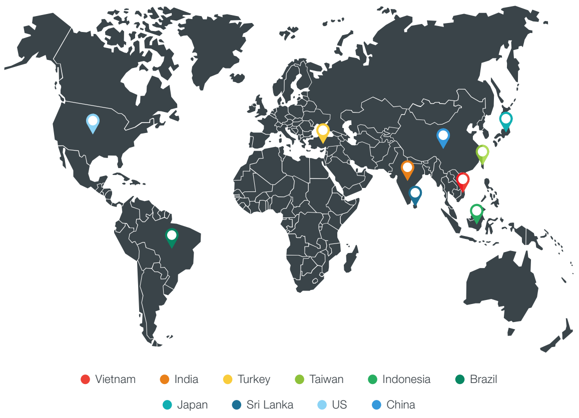


Figure 7: Countries most affected by backdoors, rootkits, and Trojan spyware

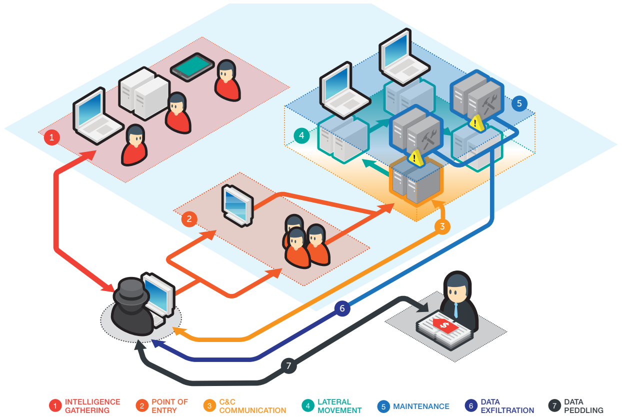


Figure 8: EsaaS attack chain

What Enterprises Can Do

Due to the nature of EsaaS attacks, securing data and shielding the network perimeter are the first steps to gain an upper hand against attackers. Network segmentation[8] and data classification, apart from system clustering according to the degree of confidentiality or importance of the information each system contains, are thus crucial in protecting company crown jewels.

Employee access to systems and servers containing highly confidential data should be limited by deploying a robust identity and access management solution with role-based access control (RBAC) and two-factor authentication (2FA). That way, only those with the right administrative levels can access highly sensitive information.

Rigorous security training for employees, particularly on risks that threats like EsaaS pose, can also help. The ability to spot spear-phishing emails can lessen their chances of serving as attack entry points.

Most of the malware that can be used in EsaaS attacks have been tried and tested over the years. They have been constantly enhanced for stealth and data-stealing capabilities. As such, enterprises need to use a connected threat defense strategy that provides maximum protection and multilayered security against sophisticated threats.[9]

This strategy combines gateway, network, and endpoint protection that:

- Shields systems, devices, and the network from known and “unknown” threats (new or improved malware versions and zero-day exploits)
- Only allows “good” (nonmalicious) files and applications to run on systems and devices
- Ensures system and network integrity by making sure that unexpected and unwanted activity is not present
- Keeps systems and devices secure even if the network perimeter is compromised
- Isolates threats detected on systems and devices so they will not compromise the entire network

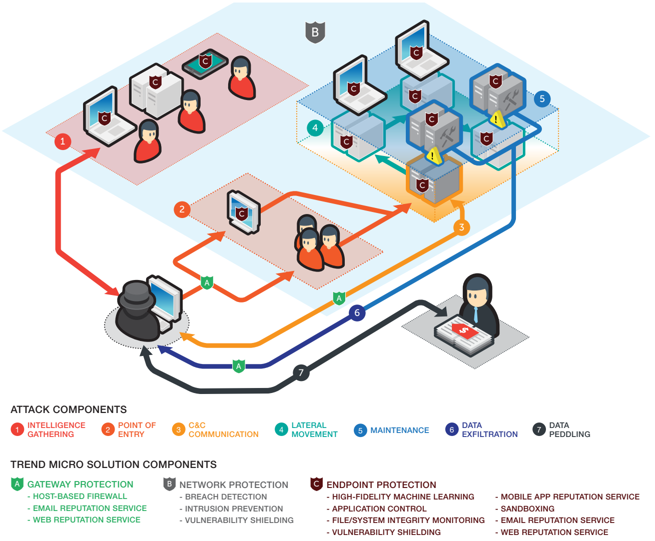


Figure 9: How Trend Micro solutions help protect against EsaaS attacks

All of the protection mechanisms above work hand-in-hand to defend enterprises from all kinds of known and unknown threats. Even as EsaaS attacks improve, enterprises remain prepared for the unknown, including zero-day exploits and new malware.

References:

[1] http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/deep-web/

[2] https://www.fbi.gov/news/stories/economic-espionage

[3] http://www.nationalcybersecurityinstitute.org/general-public-interests/cyber-economic-espionage-impacts-businesses/

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[5] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#28938ed13bb0

[6] http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/targeted-attacks/

[7] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attacks-six-components

[8] http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/protecting-data-through-network-segmentation

[9] http://blog.trendmicro.com/raising-bar-xgen-endpoint-security-protection-exactly-need/

©2016 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.