

The Rise and Fall of Scan4You

Trend Micro Forward-Looking Threat Research (FTR) Team

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.

for Raimund Genes (1963-2017)

Contents

04

Counter Antivirus Services (CAV)

05

Small Blips on the Radar

08

Scan4You's History

10

Scan4You's Admins

18

Relation to Eva Pharmacy

20

Scan4You's Resellers

21

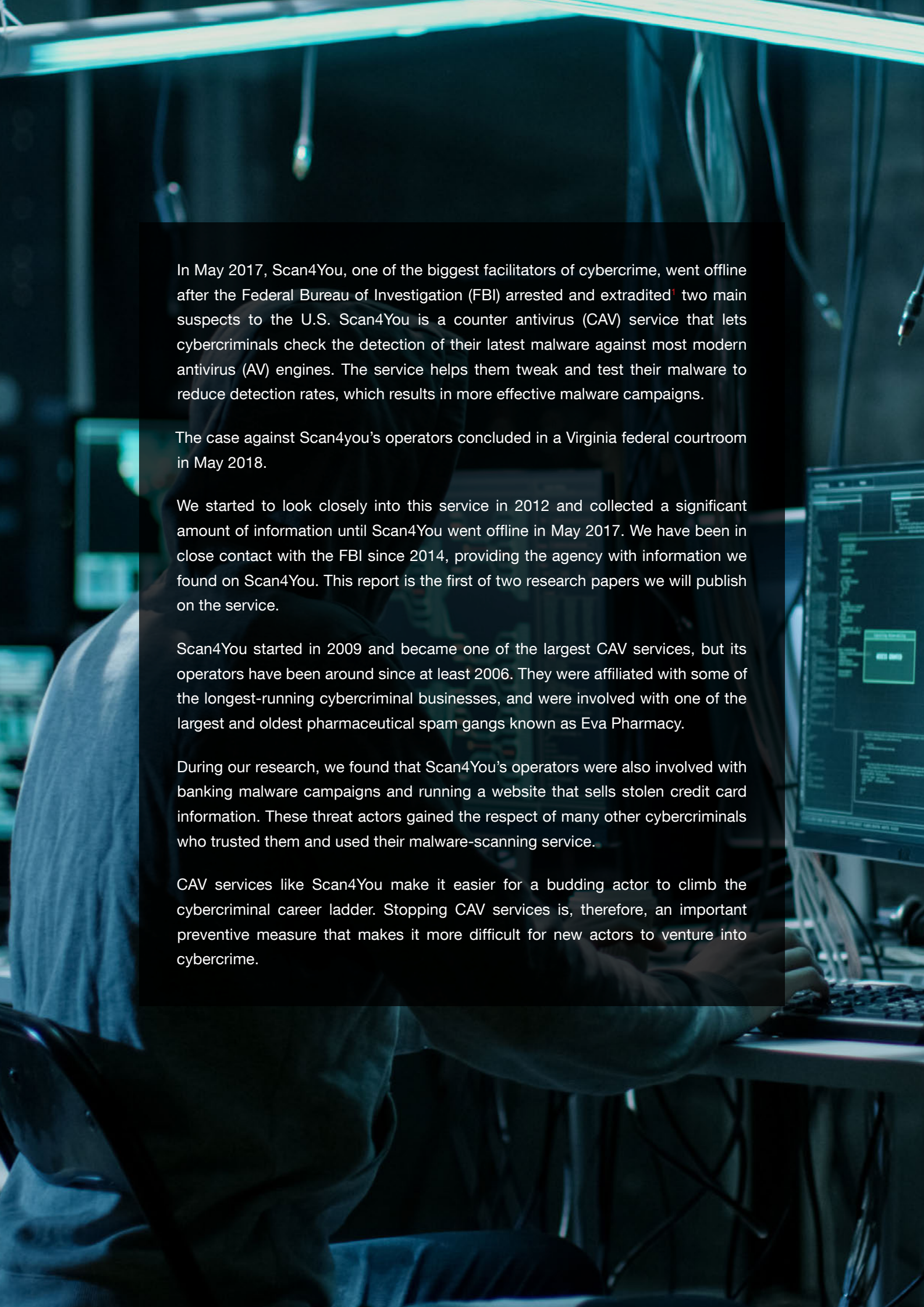
Other CAV Services

32

Impact of FBI Arrest

34

Conclusion

A person wearing a dark hoodie is sitting at a desk in a server room, typing on a keyboard. The room is dimly lit with blue light from the server racks and computer monitors. Cables are visible hanging from the ceiling.

In May 2017, Scan4You, one of the biggest facilitators of cybercrime, went offline after the Federal Bureau of Investigation (FBI) arrested and extradited¹ two main suspects to the U.S. Scan4You is a counter antivirus (CAV) service that lets cybercriminals check the detection of their latest malware against most modern antivirus (AV) engines. The service helps them tweak and test their malware to reduce detection rates, which results in more effective malware campaigns.

The case against Scan4you's operators concluded in a Virginia federal courtroom in May 2018.

We started to look closely into this service in 2012 and collected a significant amount of information until Scan4You went offline in May 2017. We have been in close contact with the FBI since 2014, providing the agency with information we found on Scan4You. This report is the first of two research papers we will publish on the service.

Scan4You started in 2009 and became one of the largest CAV services, but its operators have been around since at least 2006. They were affiliated with some of the longest-running cybercriminal businesses, and were involved with one of the largest and oldest pharmaceutical spam gangs known as Eva Pharmacy.

During our research, we found that Scan4You's operators were also involved with banking malware campaigns and running a website that sells stolen credit card information. These threat actors gained the respect of many other cybercriminals who trusted them and used their malware-scanning service.

CAV services like Scan4You make it easier for a budding actor to climb the cybercriminal career ladder. Stopping CAV services is, therefore, an important preventive measure that makes it more difficult for new actors to venture into cybercrime.

Counter Antivirus Services (CAV)

CAV services allow a cybercriminal to scan his malware against detection by various AV engines. Cybercriminals specifically set up these services to make their malware campaigns more effective. Since a malware's infection rate is naturally lower when too many AV and cybersecurity vendors detect the malware, the cybercriminal would have to tweak his malware until it doesn't get detected anymore. Some third-party services like VirusTotal also checks malware detections, but these are legitimate services that researchers and system administrators use to see if files they found on their network are malicious. These legitimate services share information with security companies, which is detrimental to cybercriminals. Hence, cybercriminals generally stay away from these services and opt to use other third-party services that do not share any data with AV companies. However, a bad actor has to place a lot of trust in a third-party CAV to use it.

Some CAV services might have started as a tool that particular cybercrime gangs initially used for their own operations. Business associates may have subsequently joined, and the service may have eventually opened to anyone willing to pay for it. It's not particularly profitable and requires a lot of work and overhead. For instance, it's difficult to manage around 100 virtual machines (VMs) installed with different AV products. They have to be regularly updated, and feedback loops have to be turned off.

Some of the more experienced cybercriminals use their own private CAV service. About a decade ago, the infamous click fraud group Rove Digital² had their own internal CAV service. The Mevade actors³ from Ukraine and Israel planned a private CAV service for their own use, but it is unknown whether they have finished it.

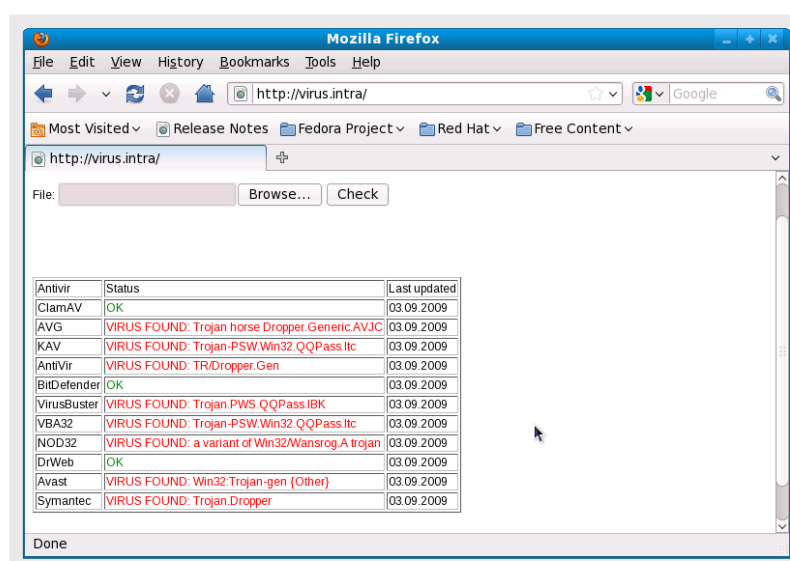


Figure 1. The internal CAV service of Estonian click fraud gang Rove Digital (screenshot taken in 2009).

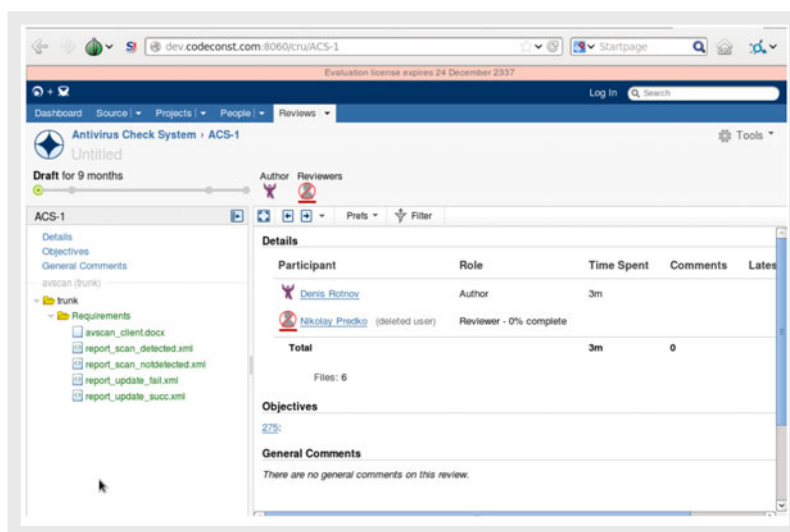


Figure 2. AV check system development of the Mevade actors.

The next sections detail our research on Scan4You, one of the most prolific CAV services. The activities of Scan4You's operators first appeared as little warning blips in the reports of the automated analysis tools on the feedback data that the Trend Micro™ Smart Protection Network™ continuously collects. A closer inspection of these led us to the unraveling of one of the largest and oldest CAV services.

Throughout our research, we were in close contact with the FBI's Washington field office. The collaboration spanned three years, resulting in the arrests of the people behind Scan4You in May 2017. These arrests made a huge impact on cybercrime, as one of its biggest facilitators was taken away. This will make future cybercriminal campaigns more difficult and expensive to mount.

Small Blips on the Radar

In the summer of 2012, we were researching an actor group that was using a private exploit kit called g01pack to spread malware. At the time, the group offered g01pack as an exploit kit for hire. The exploit kit's operators usually compromised OpenX advertisement platforms and used their exploit kit to distribute various malware. While reviewing the output of the automated tools of the Trend Micro™ Smart Protection Network™, we noticed unusual activity related to the g01pack exploits. Just minutes before the exploits were used in the wild, somebody using a couple of IP addresses in Latvia checked whether Trend Micro's web reputation system already blocked the URLs hosting g01pack's latest exploits. Each day, the same IP addresses did similar checks. A closer look showed that the corporate servers of a Latvian ISP, like the Network Time Protocol (NTP) and corporate Domain Name System (DNS) servers, were used for these checks. The IP addresses not only checked g01pack's exploit URLs but many other malicious URLs, including those that we didn't see earlier.

After this initial discovery, it did not take us long to realize what was going on. We saw a pattern among the Latvian IP addresses' many URL reputation checks: The Latvian hosts regularly checked host *testurl[.]Scan4You[.]net* against Trend Micro's web reputation system. The host was not a site that hosts anything or was on a routable IP address. It was merely used to check if Scan4You's scanning scripts still worked. We recorded this slow, steady heartbeat from Scan4you for many years from 2012 until it suddenly stopped in early May 2017.

Scan4You was an underground service that lets cybercriminals check their latest malware against more than 35 AV engines. Anybody could sign up; payment methods included Paypal, WebMoney, and Bitcoins. The price for 100,000 scans was US\$30 per month, while a single scan cost US\$0.15. Scan4You had an application programming interface (API) that made scripting easy. Scan4You's resellers, such as Refud.me and RazorScanner, also used this API. One of the service's unique selling points, which Scan4You promoted on its website, is that they do not share data with AV companies:

“This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system.”

It's an inaccurate statement, however, as domain and URL reputation checks were sent to Trend Micro's web rating servers. This is consistent with an announcement we found on Scan4You's website:

"2012-04-11 - Add Domain/IP/Url check in Trend Micro Internet Security"

The way Scan4You set up the domain, IP address, and URL checks against Trend Micro's web reputation service meant that every request will be sent to Trend Micro's rating servers. We were able to log their requests for many years and analyze the data. During limited time intervals, Scan4You also sent information on scanned files, but this feedback loop to the Trend Micro Smart Protection Network was usually turned off.

Scan4You's operators should have been aware of the fact that their service was sending a significant amount of data on scanned URLs. To our knowledge, Scan4you did not warn its users of this data sharing with us. Other CAV services like VirusCheckMate have a similar setup, but they do warn their users that URL checks will be sent to AV vendors' servers.

Scan4You's History

From 2013 – 2017, the Scan4You URL scans gave us qualitative and quantitative data that allowed us to gain insight into Scan4You's growth and success. Figure 3 indicates that Scan4You's usage started dropping from the fall of 2013 to around April 2016. Its usage picked up since then until Scan4You went dark in May 2017.

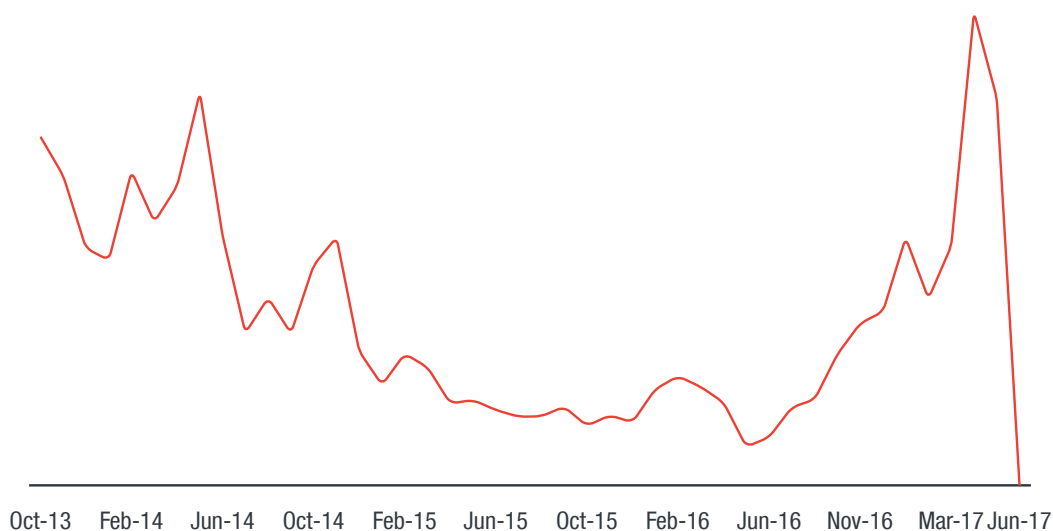


Figure 3. URL scans on Scan4You from October 2013 to May 2017. There is no scale on the vertical axis, as we don't have absolute numbers and only have sampled data

Running a CAV service is neither easy nor very profitable. Based on the scans and the pricing model on its website, we estimate that Scan4You earned around US\$15,000 per month in 2013. Scan4You has become more popular since then, and the monthly revenue may have doubled or tripled. Nevertheless, this still pales in comparison to revenue that could be earned from click fraud or internet banking fraud. It also entails running many VMs installed with around 40 regularly maintained AV software, which have to be understood. Feedback loops have to be firewalled or switched off.

Scan4You's Admins

It is no surprise that the Scan4You's administrators had ties to other, more common cybercriminal activities. It appears that they not only ran a CAV service, but they were also directly involved with one of the oldest gangs that used spam and SEO tactics to sell prescription drugs. They were also involved with the use of banking trojans and sale of stolen credit card details. We will describe more of these associations in the next sections.

Scan4You had at least two administrators: Borland and Garrik. Borland was rather careless with the way he hid his tracks while working on Scan4you and banking malware. He didn't separate his cybercriminal business from his work for a Latvian software development company. For instance, he hosted both Scan4You and Eva Pharmacy's computer servers on the corporate infrastructure of a Latvian ISP, which also hosted the software development company. He also let his family members use some of Scan4You's infrastructure to host their personal websites. The Gmail account he used to register command-and-control (C&C) domains for his banking malware contained his real name and profile photo, which he also used on his Facebook account.

Garrik's activities can be traced as far back as 2006. In 2017, he was still busy with other activities besides Scan4You. The other malicious activities we traced on the Latvian ISP's corporate servers dated back to 2007, suggesting that Garrik and Borland were already involved in cybercrime long before they started Scan4You.

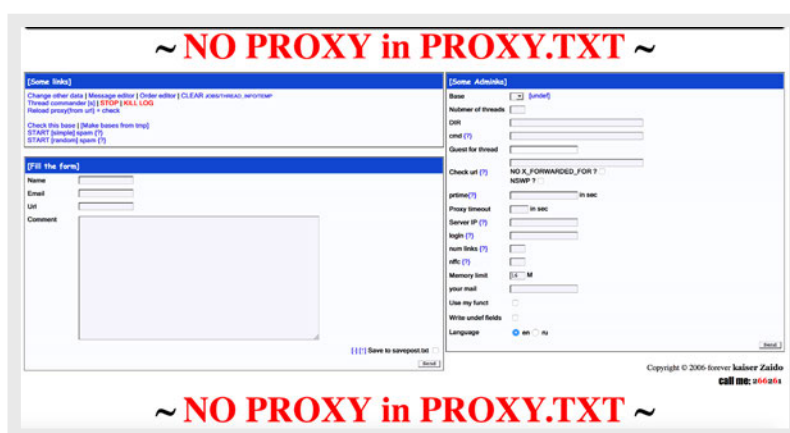


Figure 4. `hxxp://ibm[.]telenet[.]lv:80/vistamb/` hosted a guestbook spam engine in 2007, two years before Scan4You started; `ibm[.]telenet[.]lv` later became part of Scan4You's infrastructure.

b0rland/Borland

On September 22, 2009, the domain scan4you[.]biz was registered by a certain Vasiliy Kovalchuk who used the email borland@inbox.lv. We are not sure whether Vasiliy Kovalchuk is a real name. The same name was used by registrant email b0rland7@gmail.com to register C&C domain names for banking malware, specifically SpyEye and ZeuS.

Domain	Registration Date	Malware
besecure-allways[.]com	12/20/10	
bntx[.]net	12/3/10	SpyEye
deep-sec-monitor[.]net	12/20/10	SpyEye
digitazer-media1[.]com	9/4/11	
doitbro[.]com	1/13/11	
filopendere[.]com	11/29/10	
fyno[.]net	12/3/10	SpyEye
goodluck-es[.]org	1/6/10	
holdandlock[.]net	11/26/10	
indubstep[.]com	7/21/11	
luckystrike0[.]com	2/13/12	Zeus
luxuryhawaiiproperty[.]net	4/9/12	
msign[.]lv	9/13/10	legitimate
pixificator2987[.]com	4/5/11	
rainbowtechs[.]net	7/21/11	
restartwww[.]org	11/25/10	
restoration-place1[.]net	2/20/11	
restoration-place2[.]com	2/20/11	
ryahn[.]com	9/10/11	
secure-difitizer3[.]net	1/28/11	
secure-dominator[.]com	12/20/10	
secure-sleep[.]net	12/14/10	
sendspaper[.]com	12/1/10	SpyEye
sendspaper[.]net	12/1/10	SpyEye
sharedfilzz[.]com	9/10/11	
soundpong[.]com	12/1/10	SpyEye
spicemustflow[.]net	1/13/11	
terefutdd[.]org	9/10/11	
wallstreet-fucked[.]com	2/29/12	Zeus

Table 1. Domains registered by b0rland7@gmail.com.

We think that Vasilij Kovalchuk is likely a pseudonym of one of Scan4You's admins, Ruslans Bondars, who also used the handle b0rland or Borland. Regardless, Bondars very likely controlled the email address b0rland7@gmail.com. Some of the domains in Table 1 were clearly related to banking malware like Zeus and SpyEye. The domain luckystrike0[.]com was explicitly mentioned in a legal document Microsoft filed⁴ against alleged ZeuS actors on June 29, 2012.

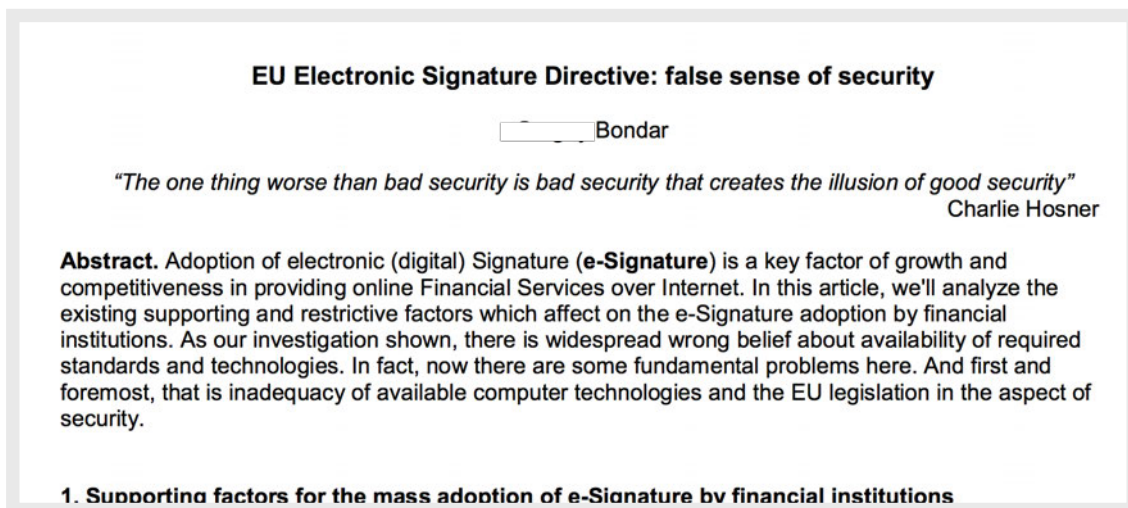
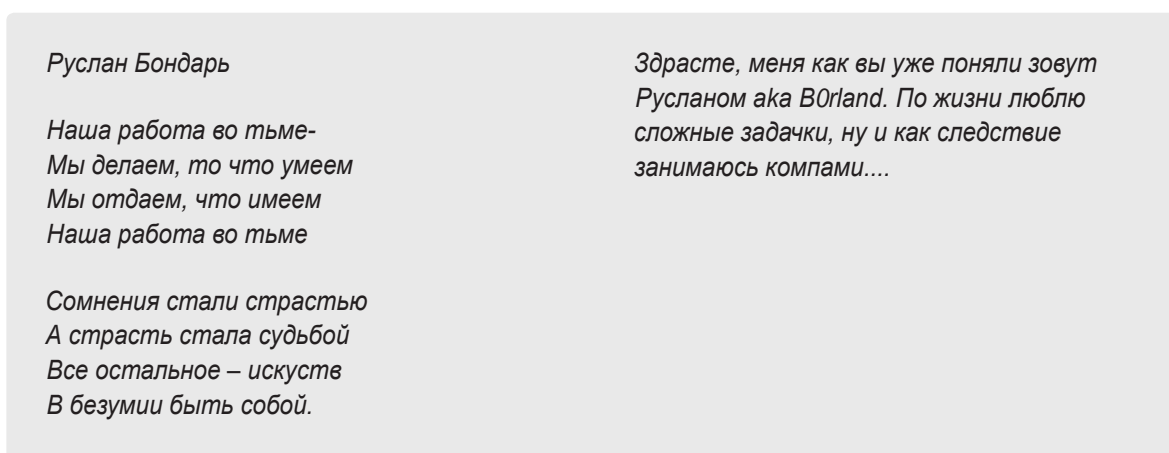


Figure 5. One of the papers was hosted on msign[.]lv.
The author is probably a close relative of Ruslans Bondars.

Ruslans Bondars registered msign[.]lv in 2010, probably for one of his family members. It hosted two documents from a relative of Ruslans Bondars in 2012. Ironically, the two documents discussed electronic signatures and "insufficient security" of online banking. Bondars also let his sister post pictures on a server called rus[.]leaping[.]net, which also hosted the source code of Scan4You's scripts and a demo page of an Eva Pharmacy website. On that personal website, Ruslans Bondars posted a poetic text from Russian science fiction author Sergei Vasilievich Lukyanenko:



Perhaps Ruslans Bondars thinks this text describes himself well. It roughly translates to:

Ruslans Bondars

*Our work in dark-
We do what we are able
We recognize that we have
Our work in the dark*

*Doubts began to passion
A passion was the fate
Everything else - the art of
In the frenzy to be yourself.*

*Good morning, I like you already
understood name Ruslans aka B0rland.
In life I like challenging puzzles, well,
as a consequence of doing Computer
Science-related things*

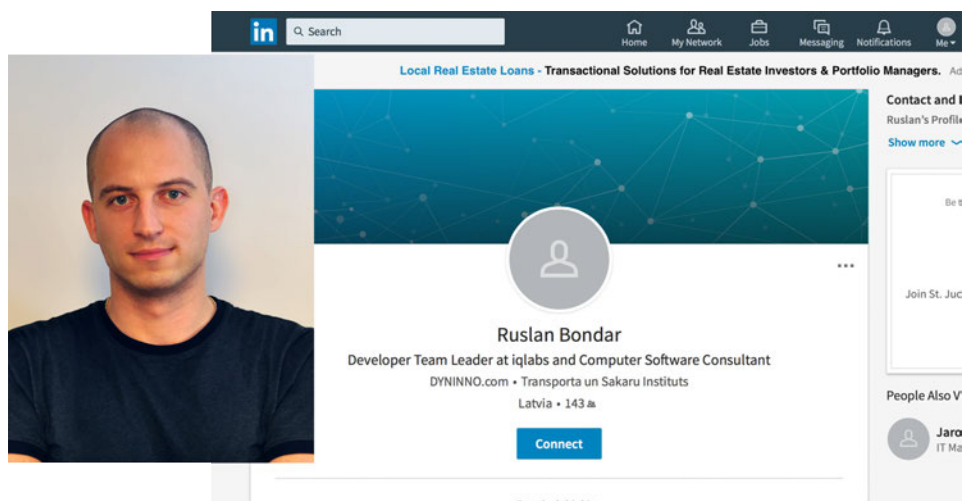


Figure 6. Ruslans Bondars in 2012 and his LinkedIn profile.

Bondars was a software developer at an internet company called Dyninno since 2005. This company is closely related to a number of websites, a particular set of which says it facilitates casting for television producers and the film industry. The casting company was fined US\$45,000 by the San Mateo District Attorney's Office in 2010 for misleading advertisements and fraud⁵.



Figure 7. Bondars at a party in New York thrown by Dyninno.

Bondars probably had access to the corporate servers of Telenet ISP in Latvia, though his resume did not indicate he worked at the ISP. Scan4You and Eva Pharmacy's operations used Telenet's corporate servers for a long time. According to Bondars's resume published on his private domain, he has Ukrainian citizenship but has lived in Latvia for a long time.

Garrik

Garrik used the email address garyaxe@inbox.lv to register more than 100 domains. Garrik used several names in the registration details, including Jurijs Martisevs and Jurijs Bereverovs. The phone number associated with Scan4You's WebMoney account matches the one indicated in the Whois data of domains registered by startolk@yandex.ru, which used the name Yury Martyshev — similar to Jurijs Martisevs. Both first names could serve as a translation of the Russian name Юрий in Latvian and English. Court documents confirmed that the nickname Garrik indeed belonged to an individual named Jurijs Martisevs.

Both email addresses belong either to the same person or to two persons who work closely together. Both registered domain names related to binary options (risky financial options prone to fraud). According to a data leak on palevo[.]biz, another CAV service advertised in 2011 in the underground, Garrik signed up with Palevo using the startolk@yandex.ru email.

Garrik also seemed to be related to a Moscow-based company that performs quality checks on concrete. The connection is odd, but it showed that Garrik had ties to Russia. Garrik had a personal blog site called garrikblog[.]com where he wrote how he left Latvia for Cyprus in April 2009 and intended to stay there for a long time. The last archived post on his blog was dated May 9, 2009.

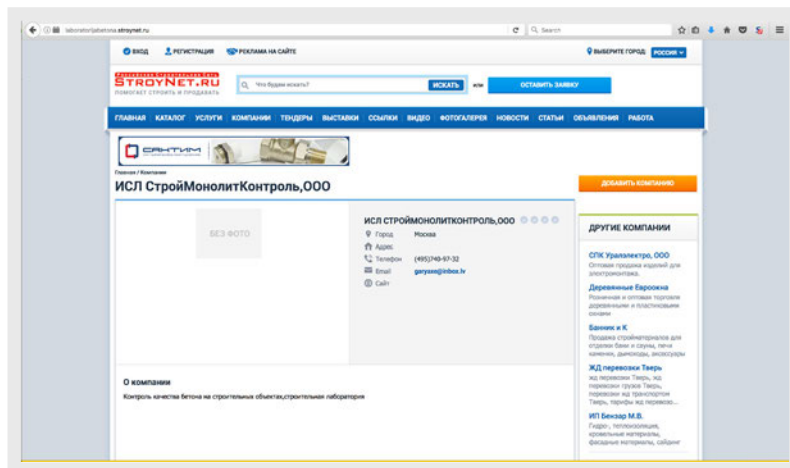


Figure 8. Garrik's email served as the contact address for a Russian company that does quality checks of concrete.

Garrik was also apparently interested in businesses that were susceptible to fraud. His interests included so-called “Binary Options” and a service that offers to write theses or college papers. Binary Options are high-risk financial options where the buyer is paid a fixed amount of money or an underlying asset when he makes a correct prediction (i.e., stock prices at certain times). He loses all money if he fails. Some consider Binary Options as gambling, and financial regulators in several countries are considering banning them. Given Garrik's past, it's unlikely he has a legitimate business here.

Domain	Registration Date	Domain	Registration Date
binaryoptionsbonus[.]xyz	11/19/15	ibinaryoptionstrading[.]xyz	12/7/15
iqbinarybonus[.]pw	11/30/15	binaryoptionstrading[.]fr	12/7/15
bestbinaryoptions[.]pw	11/30/15	ebinaryoptionstrading[.]xyz	12/7/15
binarybonusblog[.]pw	11/30/15	ibinaryoptionstrading[.]xyz	12/7/15
iqbinarybonus[.]pw	11/30/15	iqbinaryoptions[.]xyz	12/7/15
topbinaryoptions[.]pw	11/30/15	newbinaryoptions[.]pw	12/7/15
iqoptionbonus[.]pw	11/30/15	newbinaryoptions[.]xyz	12/7/15
optionbonus[.]pw	11/30/15	newbinaryoptionstrading[.]xyz	12/7/15
binarybonus[.]pw	12/1/15	iqbinaryoptions[.]website	12/9/15
10binaryoptions[.]xyz	12/7/15	iqbinaryoptionstrading[.]xyz	12/15/16
24binaryoptions[.]xyz	12/7/15		

Table 2. The registrant for all the domains above is garyaxe@inbox.lv.

Garrik also mentioned Binary Options in a post (dated December 9, 2015) on the Google+ page of his email bereverovsjurijs796@gmail.com. There, he advertised obinaryoptions[.]blogspot[.]com with a link to iqoption[.]com with affiliate ID 20867.

Domain	Registrationn Date
buyessayonline.xyz	11/10/15
primaryhomeworkhelp.org	11/10/15
apaparaphrasing.com	11/11/15
essaywritingservice.pw	11/11/15
helpwithmythesis.com	11/19/15
paperwritingservice.xyz	12/10/15
schoolofneurosciences.net	12/16/15

Table 3. Garrik is also an affiliate of fraud-prone thesis/college paper-writing services.
The registrar used here is also the same garyaxe@inbox.lv email.

Relation to Eva Pharmacy

A look into the email addresses associated with Garrik revealed ties with the infamous Eva Pharmacy group. The following Eva Pharmacy-owned domains were active in 2011 and appeared to be registered by Garrik.

Domain	Registration Data
onlinebestsite[.]com	4/9/06
ebestpharmacy[.]com	4/18/06
leadingdrugstore[.]com	4/18/06
onlinestoredirect[.]com	4/18/06
theworldpharmacy[.]com	4/18/06
toppharmacylist[.]com	4/18/06
onlinecheappharmacy[.]com	4/25/06
yourpharmasales[.]com	5/7/06
viagra-discounts[.]com	6/1/06
viagra-xenical-pharmacy[.]com	6/16/06
bettercarepharmacy[.]com	6/29/06
cheaponlinepharmacy[.]org	4/16/07
rxpharmacyonline[.]net	6/14/07
rxpharmacyonline[.]org	6/14/07
cheapcialis[.]org	10/23/08
canadianhealthcarepharmacy[.]com	11/16/09
canadianneighborpharmacy[.]com	4/22/10
menshealthonlineshop[.]com	7/2/10
canadianfamilypharmacy[.]net	7/6/10
mycanadianpharmacyonline[.]net	7/6/10
indianpharmacynoprescription[.]com	7/13/10
cheapcanadianpharmacy[.]org	8/19/10
canadianonlinepharmacynoprescription[.]org	9/14/10
canadianonlinehealthstore[.]com	9/16/10
canadianonlinedrugstore[.]org	9/20/10
internationallegalrxmedications[.]com	9/21/10
cheapcanadianrx[.]com	9/22/10
canadianpharmacywithoutprescription[.]com	1/27/11

Domain	Registration Data
onlinepharmacywithnoprescription[.]com	1/28/11
canadianhealthpharmacy[.]com	2/25/11
onlinecanadianpharmacynoprescription[.]com	2/25/11
onlinepharmacymexico[.]net	2/25/11
onlinepharmacynorx[.]org	2/25/11
onlinepharmacyonlineprescription[.]org	2/25/11
onlinepharmacyprescriptions[.]org	2/25/11
torontoonlinepharmacy[.]com	2/25/11
wiki-pharmacy[.]org	5/6/11
largestcanadiandrugstores[.]com	5/13/11
canadianpharmacynoprescriptionneeded[.]com	9/8/11
cheapcanadianpharmacy[.]net	9/8/11
cheapestcanadianpharmacy[.]com	9/8/11
drugsonlinepharmacy[.]org	9/8/11
legitimatecanadianpharmacy[.]org	9/8/11
discountdrugscanada[.]org	10/14/11
discountmexicanpharmacy[.]net	10/14/11
onlinepharmacycialis[.]com	10/18/11
onlinepharmacyviagra[.]info	10/18/11
approvedcanadianpharmacy[.]org	1/8/12
canadianpharmacyonline[.]us	2/23/12
approvedcanadianpharmacy[.]net	1/10/13
thewikipharmacy[.]com	5/14/13
thewikipharmacy[.]com	5/14/13
newcanadianfamilypharmacy[.]com	6/26/13
topcanadianneighborpharmacy[.]com	6/26/13
canadianneighborhoodpharmacy[.]com	11/20/15

Table 4. Eva Pharmacy-related domains registered by garyaxe@inbox.lv.

Domain	Registration Date
thecanadianneighborpharmacy[.]org	1/14/13
my-canadianpharmacy[.]info	1/15/13
canadianfamily-pharmacy[.]org	3/12/13
canadianneighbor-pharmacy[.]net	3/12/13
mycanadian-pharmacy[.]org	3/12/13
newcanadianneighborpharmacy[.]com	5/8/13
bestmycanadianpharmacy[.]com	6/28/13
canadadrugstoremall[.]com	7/1/13
canadafamilypharmacy[.]net	7/4/13
canadaneighborpharmacy[.]net	7/4/13

Domain	Registration Date
canadianhealthcarepharmacy[.]org	9/2/13
canadianpharmacymall[.]net	9/5/13
approvedcanadianpharmacy[.]org	7/17/14
canadianneighborpharmacy[.]org	8/26/14
torontoonlinepharmacy[.]org	8/26/14
cheapcanadiandrugstore[.]com	11/15/15

Table 5. Eva Pharmacy-related domains registered by canadnetwork@inbox.lv.

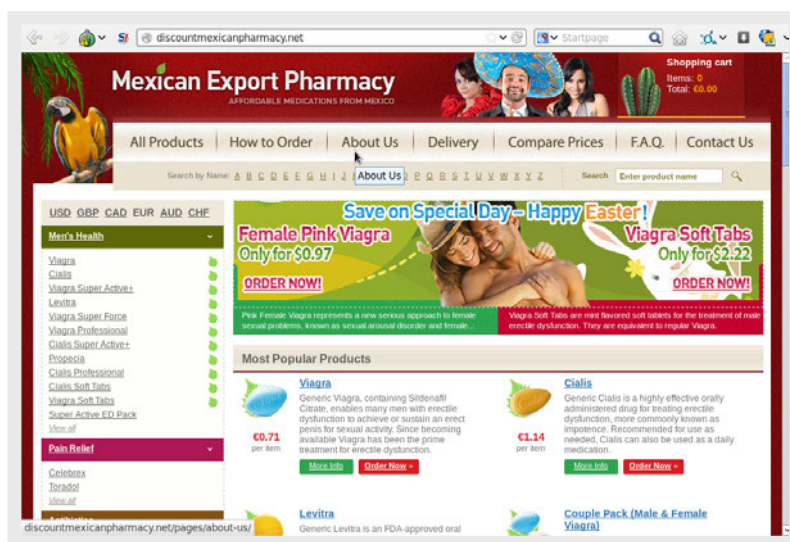


Figure 9. Screenshot of discountmexicanpharmacy[.]net in 2014.

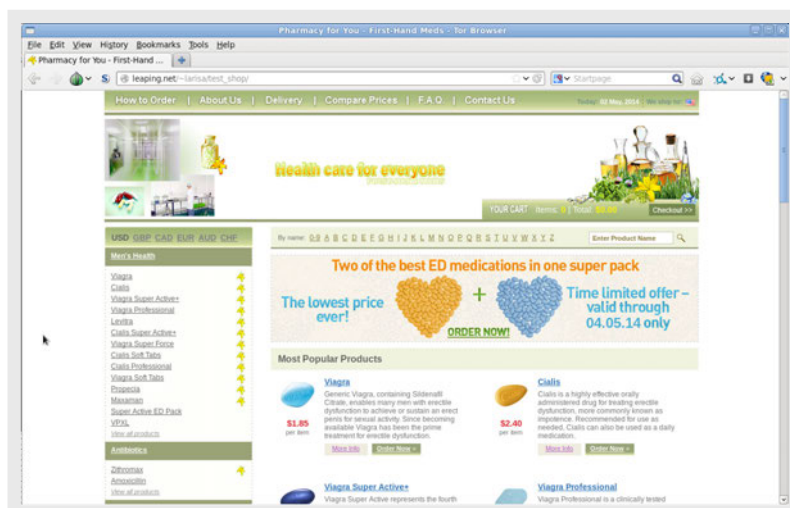


Figure 10. Test Eva Pharmacy site on Ruslans Bondars' personal domain, leaping[.]net (screenshot taken in May 2014).

Most of the domains were registered or administered by Garrik's email, garyaxe@inbox.lv. We found a test site on Borland's personal website, indicating that both were most likely involved with Eva Pharmacy.

Garrik and Borland's websites did not remain unnoticed. Some of them were mentioned in a letter issued by the U.S. FDA in 2013⁶, warning Eva Pharmacy to stop "the internet marketing of unapproved and misbranded drugs." The domain canadianneighborpharmacy[.]com was seized by the FDA in 2013 as part of a large takedown of thousands of websites that sold prescription drugs and non-FDA-approved drugs worldwide, including the U.S.

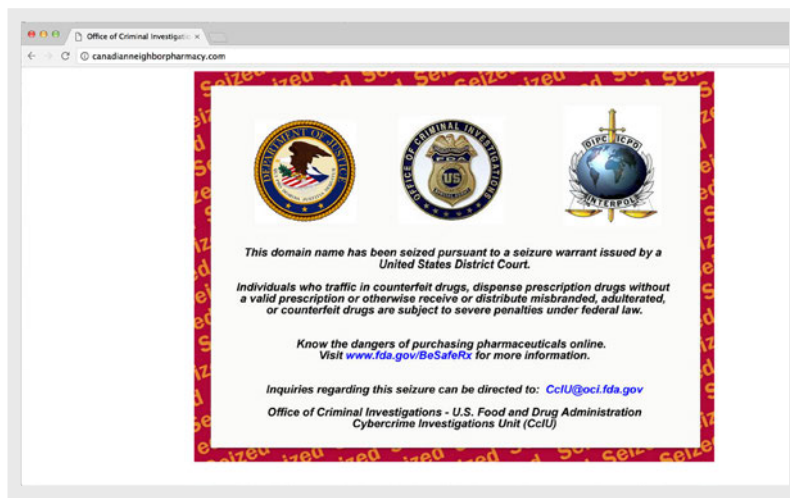


Figure 11. The FDA seized the website canadianneighborpharmacy[.]com in 2013.

Scan4You's Resellers

Scan4You was also popular among smaller CAV services that resold scanning services. Running a CAV service is a tedious task, and it's thus unsurprising that smaller players resell Scan4You's services instead. Some of these resellers provide scanning services to local, non-English markets, like Spanish or German.

RazorScanner's German owner was arrested in April 2016⁷ while Refud[.]me's British owner was sentenced to two years in prison in 2018⁸ as the result of a collaboration between the U.K.'s National Crime Agency (NCA) and Trend Micro.

CAV Service	Market
CAV Service	Market
NoDistribute	
nodetect.com	
Indetectables	Spanish users
roboservice	
RazorScanner	German users
file2scan	
Refud.me	

Table 5. Some of Scan4You's resellers.

Other CAV Services

Scan4You's main competitors were AVDetect and VirusCheckMate. Scan4You started in 2009, while AVDetect and VirusCheckMate began in 2013.

Both AVDetect and VirusCheckMate sent web rating requests to check if Trend Micro already blocks their customer's URL or domain name. The feedback we received from URL scans allowed us to compare the number of scans they carried out in 2015, as illustrated in Figure 12. Scan4You was always bigger than the other two CAV services, but VirusCheckMate also grew significantly in 2015.

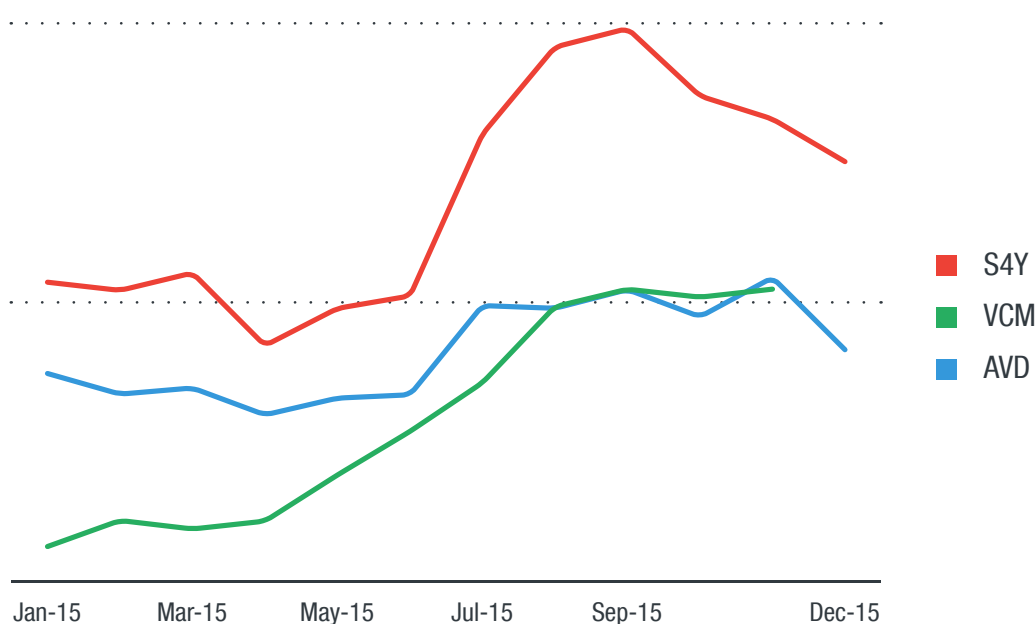


Figure 12. Comparison of URL scans by Scan4You (S4Y), VirusCheckMate (VCM), and AVDetect (AVD) in 2015

Source: Trend Micro™ Smart Protection Network™

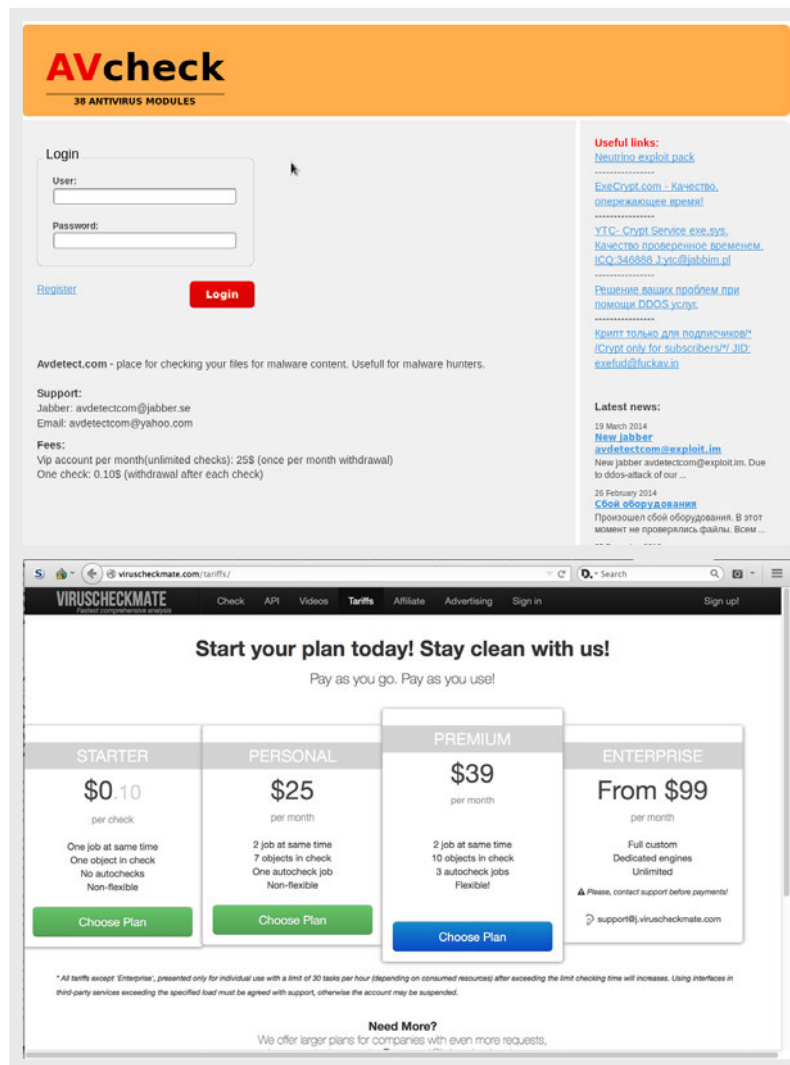


Figure 13. VirusCheckMate's website (top image) and AVDetect's website (lower image) before it went offline in 2016.

Impact of the FBI Arrest

We started looking into Scan4You in 2012 because we discovered URL scans coming from the CAV service carried out by g01pack's operators. We were in close contact with the FBI's Washington field office since the spring of 2014. We shared data and met case agents in person in Europe and the U.S. The investigation was complex and spanned about three years. In 2017, Garrik and Borland were arrested and extradited to the U.S. We noticed a significant change in the URL scans Scan4You requested to our server soon after.

On May 9, 2017, the number of new domain names scanned on Scan4You dropped to zero. We stopped receiving URL and domain rating requests from Scan4You, and the slow, steady heartbeat of `testurl[.]scan4you[.]net` being tested against Trend Micro's web reputation system went silent.

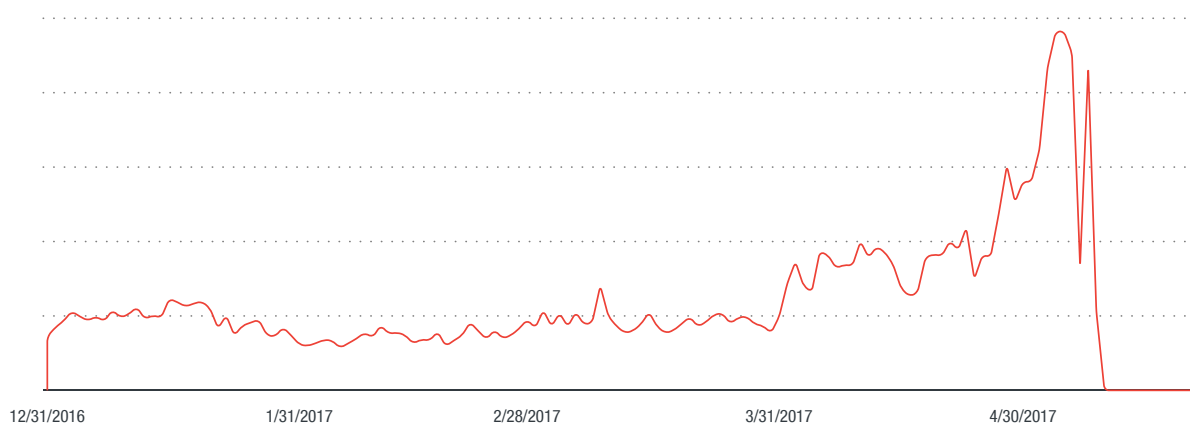


Figure 14. URLs scans on Scan4You in 2017; there is no scale for the vertical axis as we only have sampled data

The biggest CAV service ceased to operate after almost eight years, leaving VirusCheckMate as the major player. Did Scan4You's users move to VirusCheckMate? We have yet to see any significant growth in the number of URL scans coming from VirusCheckMate, which relatively stayed flat in May and June 2017. It seems most of the Scan4You's users stopped using a CAV service altogether.

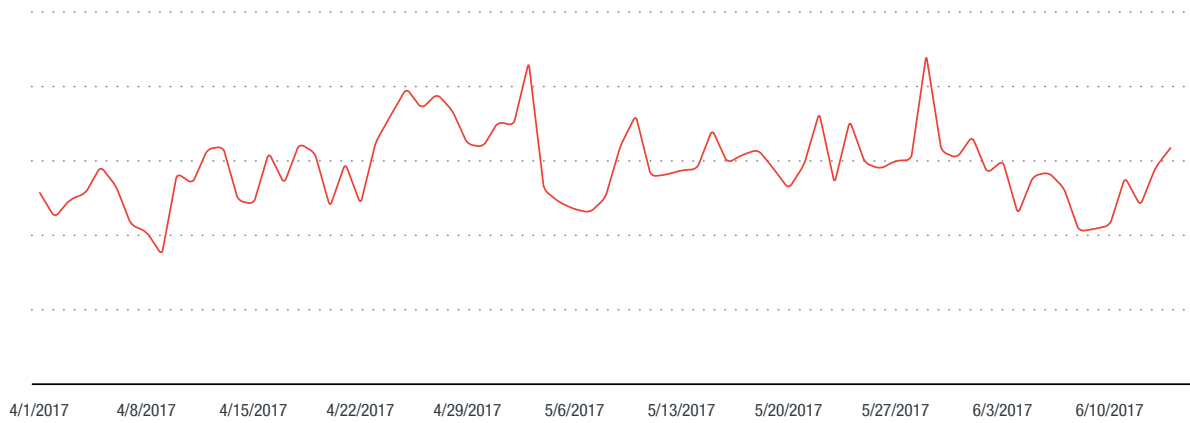


Figure 15. URL scans done on VirusCheckMate
Source: Trend Micro™ Smart Protection Network™

Conclusion

The fact that two of the main CAV services went offline in 2016 and 2017 will make it more difficult for cybercriminals to operate their illicit businesses. The arrests of Ruslans Bondars and Jurijs Martisevs, as well as Goncalo Esteves who operated Refud.me, send an important message to the cybercriminal underground.

Not only is deploying or authoring malware that victimizes innocent targets a crime; in at least some jurisdictions, so is helping others carry out these offenses. To paraphrase the press release of the Head of Operations of the NCA's National Cybercrime Unit on Refud.me, Ruslans Bondars and Jurijs Martisevs helped "hackers to sharpen their knives before going after their victims."

Indeed, with the years of work by Trend Micro and FBI that led to their arrest, we take one more step forward in securing today's connected world.

References

1. Rachel Weiner. (6 July 2017). *The Washington Post*. “Two charged with running hacking service used in ‘major computer intrusions’ of U.S. businesses.” Last accessed on 24 April 2018. https://www.washingtonpost.com/local/public-safety/two-latvians-charged-with-running-major-hacking-service/2017/07/05/17598108-6189-11e7-a4f7-af34fc1d9d39_story.html.
2. Forward-Looking Threat Research Team. (2012). *Trend Micro*. “Operation Ghost Click: The Rove Digital Takedown.” Last accessed on 24 April 2018. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_rove_digital_takedown.pdf.
3. Forward-Looking Threat Research Team. (7 July 2014). *Trend Micro*. “On the Actors Behind MEVADE/SEFNIT.” Last accessed 24 April 2018. <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-on-the-actors-behind-mevade-sefnit.pdf>
4. Microsoft Corp., FS-ISAC, Inc., and National Automated Clearing House Association v. John Does 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, icelX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petrOvich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spanishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew, and Yevhen Kulibaba and Yuriy Konovalenko. (United States District Court Eastern District of New York, 2012). Last accessed 24 April 2018. https://www.zeuslegalnotice.com/images/Amend_Compl_w_App.pdf.
5. The People of the State of California v. Casting Talent Network, Inc., dba Talent6 (The Superior Court of California, County of San Mateo, 2010). Last accessed on 24 April 2018. <https://ethanvanderbuilt.com/wp-content/uploads/2013/10/A-0000124566-1.pdf>.
6. United States Food and Drug Administration Internet Pharmacy Task Force. (26 June 2013). *U.S. Food & Drug Administration*. “EvaPharmacy 6/26/13.” Last accessed on 24 April 2018. <https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm358809.htm>.
7. Forward-Looking Threat Research Team. (15 January 2018). *Trend Micro*. “UK Conviction Arises out of Trend Micro and NCA Partnership.” Last accessed on 24 April 2018. <https://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-nca-partnership-lead-to-arrests-and-shutdown-of-refud-me-and-cryptex-reborn/>.
8. Europol. (14 June 2017). [Press release]. “International Operation Targets Customers of Counter Anti-Virus and Crypter Services: 6 Arrested and 36 Interviewed.” Last accessed on 24 April 2018. <https://www.europol.europa.eu/newsroom/news/international-operation-targets-customers-of-counter-anti-virus-and-crypter-services-6-arrested-and-36-interviewed>.



Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.



Securing Your
Connected World