Insight Space

cyber insights programme

nccgroup

Threat monitor

Threat Intelligence Report Q1 2020

A sample report from the Fox-IT Research Fusion and Intelligence Team

FOX IT

part of nccgroup

Report context

This report is a sample version of Fox-IT's quarterly insights into cyber intelligence and client-oriented threat analysis services, designed specifically to fit the needs of our managed detection and response (MDR) customer community.

This report outlines cyber threats to financial services and critical infrastructure, and supports decision-making processes and preparedness against the offensive capabilities of sophisticated threat actors and financially-motivated fraud operators.

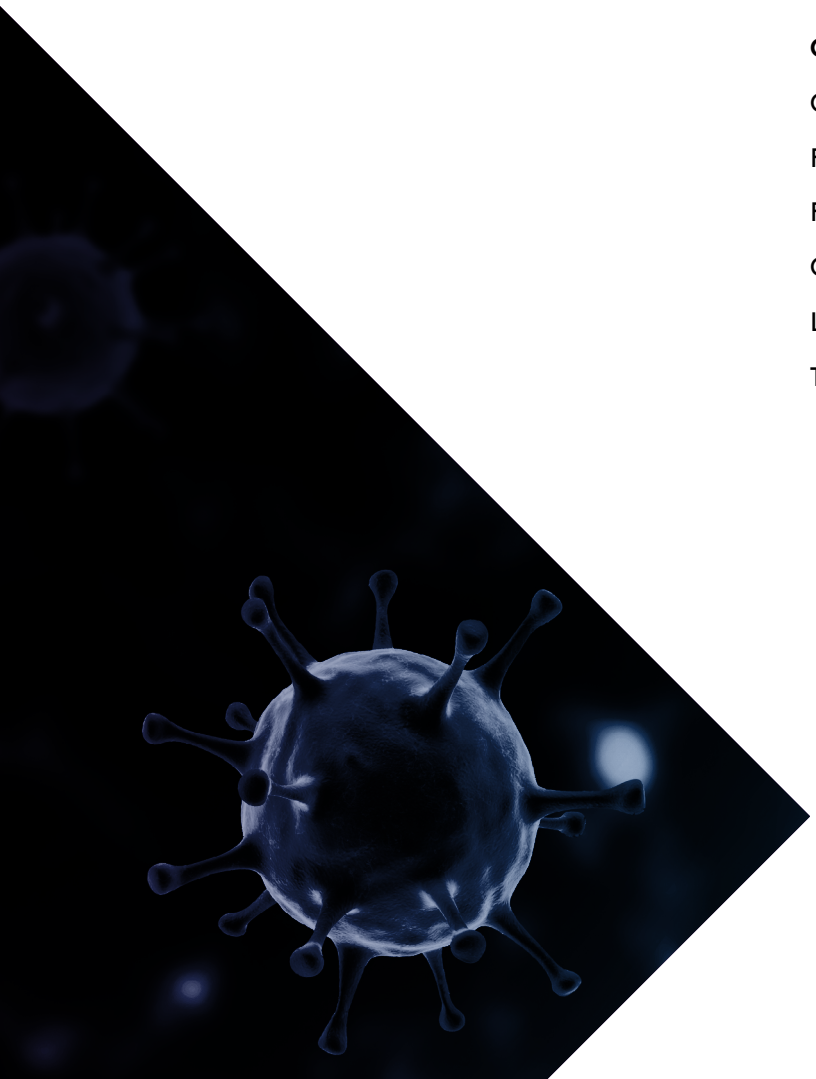
Fox-IT, as part of the global NCC Group team, believes in contributing to a more secure society, and, by offering the expertise of their Threat Intelligence team, will help to tip the scales in favour of your security teams.

COVID-19

Working on the security and availability of IT systems is perhaps more important than ever. Much of the remaining day-to-day order is highly reliant on information technology, and the presence of well-functioning IT systems in health care is therefore of vital importance.

To this end, Fox-IT has prepared and delivered customized and actionable insights for health care providers. We encourage everyone to collaborate and contribute to this cause by volunteering and sharing suspicious activity for further investigation.

Content outline



Critical events monitor

The timeline highlights the most strategically impactful incidents on the global threat landscape during this period.

All content from the below:

JANUARY

01/
Travelex forced to take digital services offline after Sodinokibi ransomware breach

14/
Microsoft patches crypto vulnerability reported by NSA

19/
Citrix releases fix for widely exploited CVE-2019-19781 in Citrix ADC and Gateway

24/
Ryuk info stealer targets government and military secrets

FEBRUARY

03/
Doppelpaymer leaks victim data on darknet if ransom unpaid

10/
Chinese Military Personnel charged with hacking Equifax in 2017 by US Justice Department

16/
Iranian Fox Kitten group exploits VPN flaws worldwide

20/
UK blames Russian GRU over 2019 Georgia defacement attacks

MARCH

05/
New PwndLocker ransomware fixes flaw allowing file recovery

09/
Compromise European power grid organization ENTSO-E restricted to office network

13/
Czech Republic hospital with Covid-19 testing laboratory hit forcing shutdown

26/
Navigator group delivers USB by post to install Griffon backdoor

COMMENTARY

The mitigation steps to reduce risk depends on the version of Citrix. Security teams at any organisations running Citrix ADC and Citrix Gateway Release 12.1 build 50.28, or those that saw a time-lapse between implementation of the mitigation steps after the release of the public exploit code on the 10th of January, should check for forensics artefacts to find indications that the vulnerability has been successfully exploited.

TAKEAWAYS

The US government has again chosen to bring criminal charges to counter actions of foreign governments in cyberspace. The unsealed indictment alleges that four officials hacked into credit reporting agency Equifax in 2017, stealing personal records such as driver's license numbers and Social Security numbers on about 145 Americans. They are members of China's armed forces, specifically PLA's 54th Research Institute. The intrusion was initiated by exploiting a vulnerability in Apache Struts software. Equifax has been faulted for lax security measures and is set to pay $380.5 million to victims of the breach as part of a class-action lawsuit.

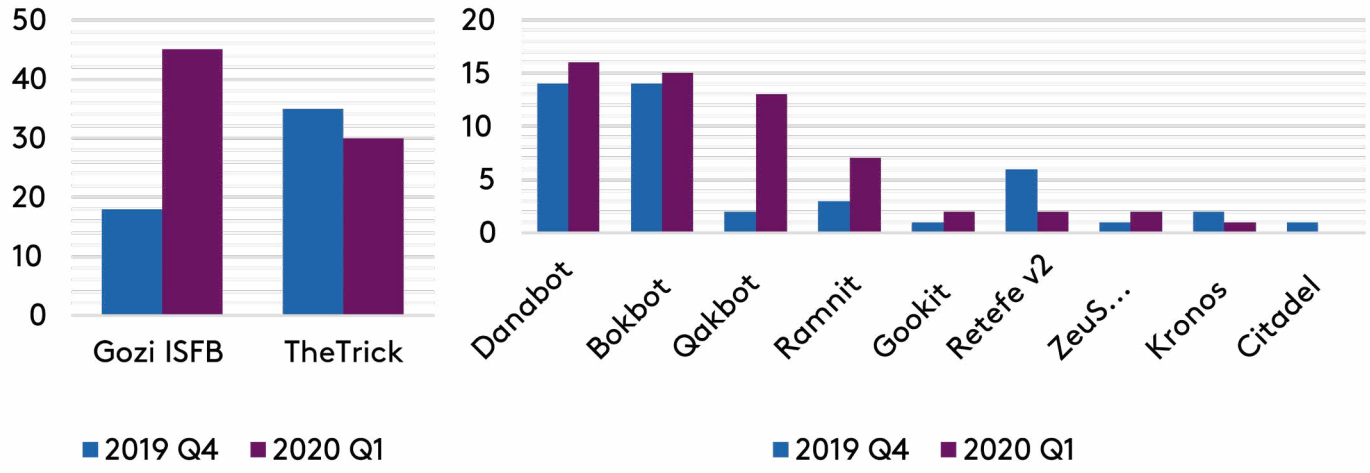
COMMENTARY

The European Network of Transmission System Operators for Electricity (ENTSO-E), a coordinating body for utilities delivering electricity, encountered malicious evidence of an intrusion into its office network. ENTSO-E stated the compromise did not spread to any operation electric transmission system impacting critical control systems. Reports indicate there was repeated, high-volume communication between a compromised mail server and threat actor infrastructure. Allegedly, the open-source Pupy RAT was used, further obfuscating the origin of the intrusion.

Fraud operators

This section outlines developments on financially-motivated attackers. The inside story on the most relevant organizational, architectural and geographical factors are detailed to enable a timely response.

Figure 4: Total target list distribution by malware family 2019 Q4 – 2020 Q1



GOZI ISFB FLYING UNDER THE RADAR

Gozi ISFB is an established name within the banking malware scene and, in terms of config distribution, is the most active banking malware family during 2020 Q1. Four different Gozi ISFB offshoots are currently widely distributed by a number of different threat actors and causing financial losses by either performing transactional fraud themselves or by facilitating other types of malicious activity.

TRW PLUS DATA BREACH

Organized crime groups carry out targeted, multi-stage ransomware attacks to lock organizations out of their critical data and information systems. Recently, invented by the Maze ransomware gang, an increasing number of TRW actors are leaking sensitive data of non-paying victims to damage organizational reputations and inflict regulatory fines as an added pressure point to force a victim to pay the ransom. Dedicated leak websites are put into production and the stolen data is subsequently released in multiple parts, leaving a line of communication open to the victim to allow them to retract the leaks upon payment.

NAVIGATOR BADUSB ATTACK

FIN7 – tracked by Fox-IT as Navigator – is a threat group involved in high volume credit card theft and notorious for its use of crafty social engineering techniques to obtain a foothold within target networks. Recently, and fitting the group's modus operandi, Navigator distributed a malicious USB thumb drive, including a gift card and letter to victims in order to deliver the Navigator GRIFFON backdoor. The USB exploit is known as 'BadUSB' and acts as an USB keyboard to inject malicious commands, more specifically to retrieve two pieces of PowerShell code.

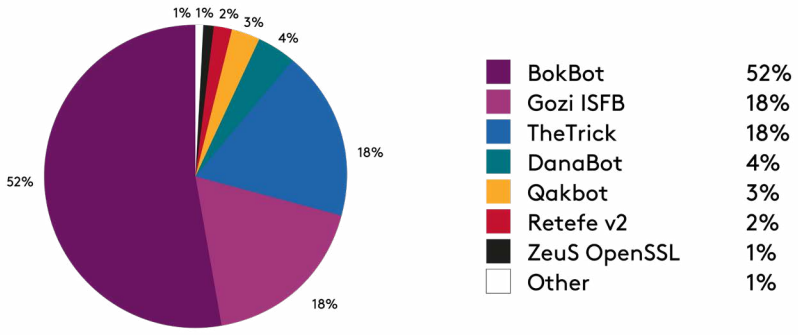
Financial malware trends

The financial sector and online payment systems specifically are a continuous target of fraud attacks by financially motivated hacking. The malware tailored to exploit the online banking processes known as banking trojans are detailed over time to capture trends and patterns.

TROJAN ACTIVITY

Bokbot is responsible for the majority of malicious activity, and is continuing its proven approach of targeting North American financials while updating its functionality at the same time. Although TheTrick is mostly moving away from wire fraud, the group is still responsible for a fair amount of global activity. Growth is again observed for both Danabot and Gozi ISFB, with the latter initiating new worldwide campaigns.

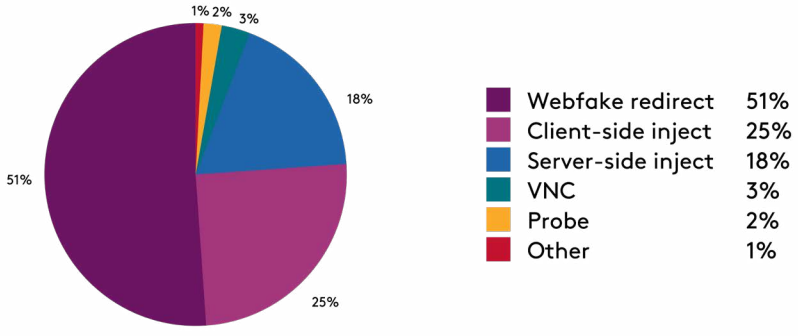
Figure 1: Threat size of financially motivated threat actors 2020 Q1



ATTACK TYPES DEPLOYED

When it comes to banking trojans, webfake redirect attacks are often deployed as the weapon of choice in order to commit fraud, in which victims are redirected to a phishing page representing the online banking page. For the client-side webinject, bank interfaces are adapted with an overlay to illicitly access credentials and mislead users during transfers. Overall, server-side inject attacks are decreasing and are solely deployed by TheTrick group to selective targets.

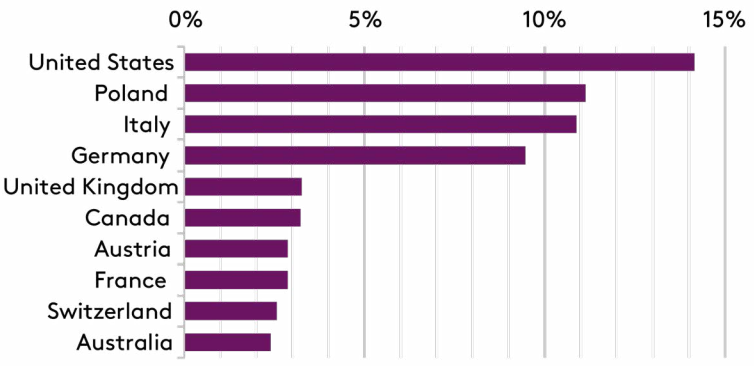
Figure 2: Attack types leveraged by financial malware 2020 Q1



TARGETING BY COUNTRY – TOP 10

Attacks are primarily concentrated in Europe and North America, again representing a continuation of the previous quarter. Both Poland and Italy are increasingly scoped for exploitation, the US however remains the overall top targeted country. Note that the Top 10 countries amount to more than half of all targeting: for 2020 Q1 up to 63% and for 2019 Q4 as much as 69%.

Figure 3: Top 10 targeted countries by financial malware 2020 Q1



Credit card recovery

During the first quarter of 2020, Fox-IT recovered over 700,000 compromised cards originating from the source codenamed “Octopus”.

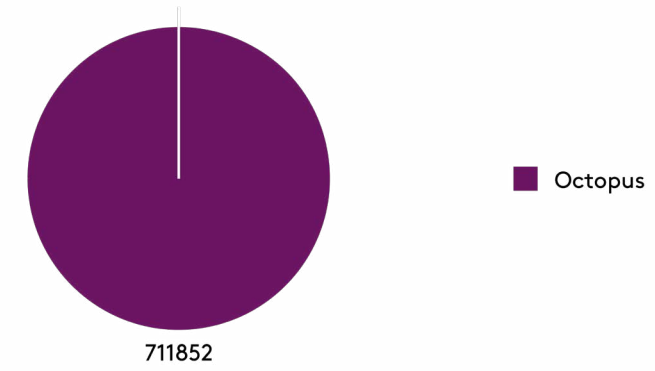
Octopus was however subject of a Russian law enforcement operation in March this year, which effectively cut off our visibility. New sources for credit card data are however uncovered and subsequently prepped for distribution.

700,000

Compromised cards recovered

On the 20th of March the Russian FSB initiated a takedown operation on a credit card theft ring Fox-IT refered to as “Octopus”. Octopus is essentially a platform that hosts a large number of carding shops selling credit card track data. We have written extensively about Octopus in our Threat Monitor Annual Report 2019. According to our insights the entire infrastructure has been taken down and thus we are no longer able to provide cards from this source. Further information is detailed in the section below.

Figure 5: Count of recovered cards by source



Law & enforcement

Here, primary law enforcement and legislative actions impacting cyberspace are summed up. Most significant are operations that have an immediate impact on active threat actors and the infrastructure, malware and monetization channels they leverage.

RUSSIA BLOCKS SECURE EMAIL

The Russian government is increasingly blocking access to secure email services such as ProtonMail, Tutanota Mail and Startmail. Shifting more and more towards China's model of internet censorship, Russia's state communications watchdog "Roskomnadzor" is through legislation now allowed to control information and block (messaging) applications. This signals new important steps towards an indepen-dent Russian internet not reliant on routing through other countries.

OCTOPUS TAKEDOWN OPERATION

On March 20th, 2020 the Russian Federal Security Service (FSB) arrested 30 individuals that were involved in a high volume credit card data theft and distribution network Fox-IT referred to as "Octopus". Russian law enforcement action on cybercriminals residing within its own borders is exceptionally rare, however, according to our insights (confirmed by the FSB statement) the group sold card data originating from both Russian and foreign financials thus revealing a potential motive.

CORONA CRIMINALS PRIORITIZED

The current COVID-19 pandemic provides cybercriminals with ample opportunity to exploit these unprecedented times for various nefarious means. Several governments are considering their options to combat this malicious activity, e.g. with the U.S. prioritizing the prosecution of cybercriminals exploiting fears about the corona virus. The Australian Signals Directorate stated that it had "mobilized its offensive cyber capabilities to disrupt foreign cyber criminals responsible for a spate of malicious activities during COVID-19", advertising its hacking potential.

Understanding the objectives and methods of threat actors is key to building a stronger security strategy.

Our experts are always here to help your organisation become more resilient - if you have any questions about any of the content in this paper, or would like to access the full version of this report, please contact your account manager.

Terms of use

Fox-IT tracks global cybercrime activity. We base our intelligence on tracking threat actors, darkweb research, forensic investigations, internationally deployed sensors and fraud monitoring services.

Going beyond botnet & malware information, we provide a global picture of trends, geographical activity, actors, their motivations and their evolving business models. We provide links to campaigns, tactics, procedures and individual IoCs to feed network security components. Customers become part of a global community, with live threat tracking, collaboration, and the largest criminal threat database, with over a decade of experience.

The data and charts contained within this report represents Fox-IT its own dataset collected within its malware lab. The data from this lab should be considered a sample including factors potentially skewing the analysis: our lab does not analyze every malware sample on the threat landscape, merely those assessed to represent a cross-section from a variety of sources. Our sources may be skewed towards certain types, families or regions which can introduce further bias. The report documents the dataset over a fixed period of time allowing for comparative analysis, whereas when referring to previous datasets a discrepancy with previous reports may seemingly occur due to inclusion of the updated dataset that may contain recent data impacting the statistical outcome.

Furthermore, the lists of data we use to identify targets for attacks can also be biased because they will naturally contain more data pertaining to Fox-IT customers than organizations not part of the MDR community. Although we augment customer supplied data (such as URLs for online banking and BINs) with autonomously collected data, the customer supplied data will always be more detailed and extensive. In short, these charts provide indications, and should be incorporated by interested parties as such. Customers are advised to incorporate and correlate multiple feeds with internal network telemetry.

nccgroup

Insight Space

cyber insights programme

FOX IT
part of nccgroup

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

www.nccgroup.com

Fox-IT

Founded in 1990 as a consultancy firm for forensic expertise, their headquarters are in Delft, Netherlands and is at the heart of NCC Group's Threat Intelligence Research Fusion Centre. Fox-IT solves and mitigates the most serious threats caused by cyver attackes, data leaks or fraud with innovative solutions for governments, defence agencies, law enforcement, critical infrastructure and banking, and commercial enterprise clients worldwide.

For more detailed information about Fox-IT, including partner details, please go to

www.fox-it.com