From Russia…With Love?

Part 1: Background

Introduction

The symbiotic relationships between the Russian government and individuals associated with organized cybercrime groups within its borders are becoming increasingly problematic for the international community. The Russian government's current stance is to largely ignore criminal targeting of Western states and businesses, inhibiting meaningful international response to the rise of ransomware attacks across many industry verticals, including state, local, tribal, and territorial (SLTT) governments and the critical infrastructure assets they operate.

Key Findings

- The Russian government's varying and complex relationships with Russia-based cybercriminals are not new, but are proving increasingly difficult to ignore. Due to these relationships and the legal hurdles facing international criminal prosecution of Russian criminals, it is unlikely that individuals associated with cybercrime activity will be extradited from Russia in the near-term. However, cybercriminals that travel to countries with extradition agreements with the West are at a greater risk of being arrested and extradited to the United States.
- Russia's tense relations with the United States and members of the North Atlantic Treaty Organization (NATO) not only make extradition an unlikely solution, but very likely encourage ransomware gangs and other cybercriminals to continue targeting Western organizations without fear of consequence.
- Due to the frequency, scope, and growing sophistication of ransomware threats, it is highly recommended that MS-ISAC members, especially those overseeing any critical infrastructure, audit and pursue a robust security posture using resources listed in part 2 of this post.

Background Information

Reports detailing the Russian government leveraging cybercriminal entities date back to the late 1990s when the FSB (Federal'naya Sluzhba Bezopasnosti), Russia's domestic intelligence and security service, coerced cybercriminals to act as internal proxies to deface pro-Chechen websites.[1] One forerunner to the current cybercrime scene was the Russian Business Network (RBN). The RBN was a loose conglomerate of web-hosting companies that leveraged network peering agreements to route network traffic to and from the undesirable content it hosted, including pirated films, child pornography, phishing sites, and malware command and control (C2) servers. The RBN appealed to cybercriminals, as almost all abuse reports concerning malware C2 infrastructure were largely ignored by companies comprising the greater RBN.[2] In his book, *Spam Nation,* journalist Brian Krebs details the FSB's awareness of the RBN and acceptance of protection money from its leadership to continue operating unabated.[3] The RBN also hosted active malicious infrastructure targeting Georgian government websites during the Russian military incursion into Georgia in 2008.[4] Despite the RBN being severed from many upstream internet providers in late 2008, its business model still serves as an example for bulletproof hosting services.

During the same period in the early 2000s, the Zeus banking trojan emerged and signaled the commoditization of the cybercriminal underground. Evgeniy Bogachev—also known as Slavik in criminal forums—is a key individual who helped shape the current cybercriminal threat landscape.[5] In 2006, Bogachev created and began selling Zeus as a user-configurable banking trojan. Zeus quickly gained popularity on criminal forums due to the method it used

to steal banking credentials. Upon infecting a host machine, Zeus would embed malicious JavaScript into a victim's web-browser to alter banking websites as they loaded into a victim's browser—also known as webinjects. When an infected victim navigated to a targeted banking website listed in the malware's configuration, the browser-embedded webinjects would collect user-entered login credentials and then siphon them off to an external server for future sale or exploitation. Although the Zeus source code was leaked in 2011, the code still remains a popular codebase for crimeware kits. The MS-ISAC continues to regularly observe Zeus-related signatures in our top five malware families detected via Albert sensors.

Bogachev also worked with a smaller group of cybercriminals known as the Business Club to create a more effective and exclusive malware strain based off of Zeus.[6] This strain became known as JabberZeus due to its utilization of the instant messaging protocol Jabber, which would alert Business Club members when a victim logged into their account. The Business Club would ultimately grow JabberZeus into a sophisticated, peer-to-peer variant dubbed Gameover Zeus.[7] The peer-to-peer functionality of Gameover Zeus was highly resistant to takedown efforts by incorporating protocols for infected machines to fetch information from one another instead of communicating back to centralized command and control servers.

Figure 1: FBI Wanted poster for Evgeniy Bogachev

The Business Club also concealed its success from international law enforcement by leveraging money mule networks, and allowed others access to Gameover Zeus infrastructure only if they entered into profit-sharing agreements with the core group. It is estimated that the Business Club stole tens of millions of dollars in just a few short years, with estimates ranging greater than $100 million from the Zeus enterprise as a whole.[8] Security researchers discovered several Gameover Zeus bots possessing capabilities outside of traditional banking malware. For example, a sample found in Georgia was configured to search for files related to counterintelligence operations and key government personnel. A bot in Turkey probed government networks for any intelligence on Russia's activities in Syria, while another bot in Ukraine scavenged for anything related to Russian intelligence activities in Ukraine.[9]

In 2014, the Gameover Zeus botnet was dismantled by a joint effort between security researchers and international law enforcement.[10] Soon after the dismantling of Gameover Zeus, Dyre (also known as Dyreza) appeared, mimicking many aspects of Gameover Zeus, including sharing a similar banking target set, webinject code, as well as using the same downloader module.[11,12] In 2015, however, the operators behind Dyre were raided by Russian authorities. The FSB refused to comment on the matter, with one security firm noting that Dyre did not pursue any Russian targets.[13] The reasoning behind this takedown remains unknown to public sources. Despite the sinkholing

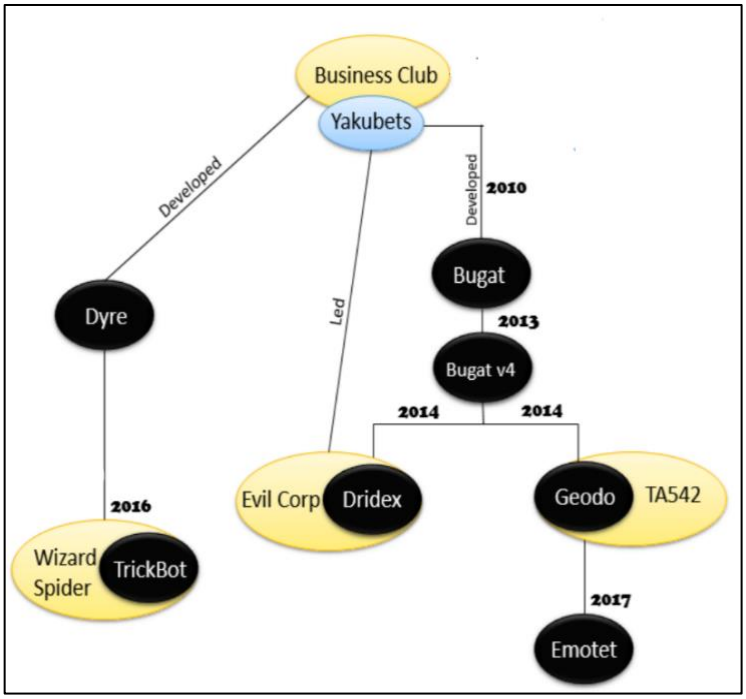

Figure 2: Diagram of malware after the Gameover Zeus takedown. Source: French CERT

of Gameover Zeus and Dyre, malware like TrickBot and Dridex emerged in their wake and continue to showcase that sophisticated cybercriminal operations occasionally intersect with Russian state interests. TrickBot originated as a banking malware but morphed into a modular "do-it-all" malware, tracing some of its code-lineage to Zeus and Dyre.[14]

In fall 2020, U.S. Cyber Command and Microsoft Corporation conducted separate takedowns of TrickBot infrastructure to reduce the likelihood of TrickBot acting as a loader for a potential ransomware attack on election-related infrastructure. Microsoft assessed that a ransomware attack on a key election district would have indirectly supported Russia's goal of delegitimizing an already polarized 2020 U.S. presidential election.[15] Further highlighting Russian cybercriminals' comfortability from prosecution, an indictment of a TrickBot developer arrested in Miami in February 2021 cites an internal chat log where the operators were quoted in 2016 saying "They should say thank-you to us that we're stealing money from the Americans; we should get the Medal of Valor."[16]

The banking malware Dridex emerged in 2014 and is thought to be authored, at least in part, by former Business Club member Maksim Yakubets.[17] Yakubets is also believed to lead Evil Corp, a notorious cybercrime gang connected to several major strains of ransomware that, by one estimate, have netted hundreds of millions of dollars in profit[18,19]. Yakubets and Evil Corp were targets of a 2019 U.S. Department of the Treasury sanction, which stated that "Yakubets was in the process of obtaining a license to work with Russian classified information from the FSB." "Yakubets was tasked to work on projects for the Russian state, to include acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf."[20]

A 2021 U.S. Department of Justice indictment explicitly describes Evil Corp and the Russian government's ties, stating that "the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns."[21] Interestingly, Yakubets is also married to the daughter of Eduard Bendersky,[22] a successful high-ranking former FSB Vympel officer who heads a private military organization responsible for a proxy assassination in Germany in late 2019.[23]

Figure 3: FBI Wanted poster for Maksim Yakubets

Separate from the large botnets like TrickBot and Dridex, the FSB also recruited two Russia-based cybercriminals in 2014 to target Yahoo! and gain information on Russian journalists critical of the government, as well as U.S. government personnel of interest. Beginning in January 2014, "Dmitry Dokuchaev and Igor Sushchin, protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the U.S. and elsewhere. ... they worked with co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals" to include Russian journalists and U.S. government officials.[24] The breach ultimately affected between 500 million and one billion users and caused Yahoo! to recommend that millions change their passwords as a remediation.[25]

This is the end of part 1. View the From Russia...With Love Part 2

References

1.) https://www.nytimes.com/2000/06/29/technology/in-bleak-russia-a-young-man-s-thoughts-turn-to-hacking.html

2.) "RBN" in this sense encompasses the entire operation, whereas there was an actual hosting provider called "The Russian Business Network"

3.) *Spam Nation,* Brian Krebs

4.) https://www.nytimes.com/2008/08/13/technology/13cyber.html

5.) https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

6.) https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

7.) https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf

8.) https://krebsonsecurity.com/2015/08/inside-the-100m-business-club-crime-gang/

9.) https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf

10.) Ibid.

11.) https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates/?sh=7337b4bb2a0a

12.) https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

13.) https://www.bankinfosecurity.com/report-dyre-crackdown-in-moscow-a-8853

14.) https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

15.) https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

16.) https://www.justice.gov/opa/press-release/file/1401766/download

17.) https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets

18.) https://www.accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware

19.) https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

20.) https://home.treasury.gov/news/press-releases/sm845

21.) https://home.treasury.gov/news/press-releases/jy0127

22.) https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.html

23.) https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/

24.) https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

25.) https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html