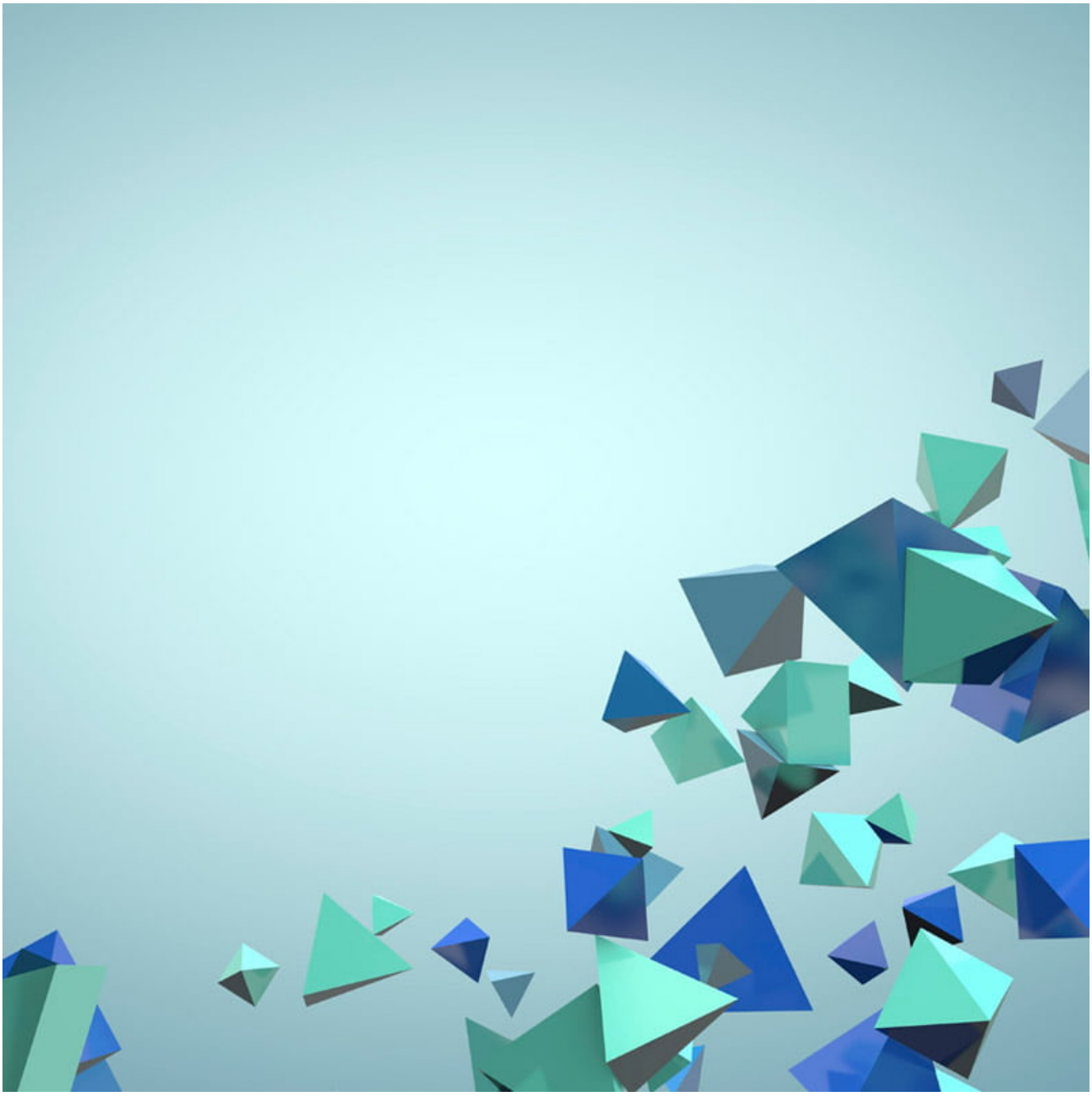
Evolution of the GOLD EVERGREEN Threat Group

secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

Secureworks Counter Threat Unit



Summary

SecureWorks® Counter Threat Unit™ (CTU) researchers analyzed the evolution of GOLD EVERGREEN (also known as Business Club), an Eastern European threat group known for large-scale, financially motivated electronic crime. Over time, the threat actors have demonstrated a high level of organization, a wide range of criminal activity, and the ability to

steal significant amounts of money. Many of the same threat actors have been involved with the different incarnations of the group for more than 15 years, and they used various malware families to achieve their goals. The adaptability to enhanced fraud controls and infrastructure takedowns demonstrates GOLD EVERGREEN's resourcefulness, sophistication, and resilience.

Background

GOLD EVERGREEN evolved from the Eastern European threat group Rock Phish (also known as the Rock gang), which was active from 2004 to 2008. The Rock Phish name is based on strings in the group's phishing URLs. Its large-scale and geographically focused phishing campaigns impersonated several banks using multiple phishing sites hosted on the same infrastructure. In early 2007, Rock Phish was one of the first threat groups to use fast-flux DNS on a large scale. It also used a centralized collector system to send stolen credentials through layers of proxies and collect them in a central database hosted on a bulletproof infrastructure. Standard phishing kits were vulnerable to hijacking because they were easily backdoored or they stored stolen credentials with world-readable permissions.

In late 2008, the Rock Phish threat group incorporated the Asprox botnet into an upgraded infrastructure. The evolution to hosting phishing sites on a botnet of compromised home computers rather than on compromised websites or purchased infrastructure made the compromised systems much more difficult to seize or take down. Centralized backend collectors located in Eastern Europe were used with globally distributed proxies. While this botnet and hosting platform were used for other criminal activity, it was Rock Phish's phishing attack style and use of the botnet that earned notoriety. However, the activity was attributed to the Avalanche threat group.

In a 2009 report, the Anti-Phishing Working Group (APWG) named Avalanche "the world's most prolific phishing gang" and deemed it "responsible for two-thirds of the phishing attacks launched in the second half of 2009." CTU™ researchers assess it is highly likely that many of the Rock Phish threat actors moved to the Avalanche hosting network to improve their phishing activity. Most of the Rock Phish threat actors were of Ukrainian and Russian origin, with reported Romanian and Moldovian involvement. Due to the limitations of law enforcement and cybercrime investigative capability in 2009, there were no arrests or indictments of Rock Phish or Avalanche threat actors. As the Avalanche network grew, it became a popular hosting platform for many criminal enterprises until November 2016, when it was dismantled and its administrators (including Ukrainian Hennadiy Kapkanov) were arrested after a four-year investigation. Kapkanov appeared before a Ukrainian court but was released, and his location is unknown as of this publication. The threat group evolved into GOLD EVERGREEN when it began using Gameover Zeus for its activities.

Related malware

Over the years, the threat group used different malware families to conduct their activities. Some of the malware families shared code and infrastructure.

Zeus and Jabberzeus

The Zeus information-stealing malware created by Evgeniy Bogachev (also known as Slavik, A-Z, Pollingsoon, and Lucky12345) was first observed in late 2006. Zeus offered advanced functionality such as dynamically interacting with bank websites, not requiring lookalike phishing domains (which required registration and were subject to takedown), and providing keylogging to steal a wide range of credentials. It was distributed via the Avalanche infrastructure in late-2009, but the volume of Avalanche phishing attacks dropped significantly by mid-2010 (see Figure 1). CTU researchers assess that the Avalanche threat group tested the Zeus malware using the Avalanche hosting infrastructure and then switched to distributing Zeus directly via email messages, causing the drop in observed phishing attacks.

Month	Avalanche Attacks	Domain names
July 2009	12,793	498
August 2009	16,372	603
September 2009	18,633	656
October 2009	26,411	924
November 2009	7,089	523
December 2009	2,952	959
January 2010	2,028	877
February 2010	2,024	531
March 2010	146	145
April 2010	59	59
May 2010	11	8
June 2010	4	4

Figure 1. Avalanche phishing attacks between July 2009 and June 2010. (Source: APWG)

By leveraging Zeus, the Avalanche threat group increased earnings and diversified its activities. The group rented the Cutwail spam botnet in early 2010 to send spam emails containing Zeus attachments. The transition to information-stealing malware was pragmatic because stolen credentials resulted in fewer successful fraudulent transactions as banks increased their fraud controls. New solutions were needed for criminals to bypass challenge questions and fraud detection based on IP addresses in specific geographic locations.

Around mid-2009, suspected Avalanche members worked with Zeus trojan creator Bogachev to develop a customized version. Jabberzeus incorporated the Jabber communication protocol to notify threat actors when a victim logged into their online banking account. SecureWorks reported that banks lost approximately $100 million in 2009 due to the Jabberzeus botnet. The Avalanche threat group used it in conjunction with the Leprechaun private inject framework (see Figure 2) to automate fraudulent transactions on Internet

banking platforms. Leprechaun was likely developed by Alexey Tikonov (also known as Kusanagi and Kusunagi), whom Microsoft also named as a coder and inject writer involved with Zeus in its 2012 John Doe lawsuit. The Leprechaun framework was highly customizable and allowed threat actors to write web injects for each targeted organization. The web injects could be customized to each victim's online experience and could anticipate security and anti-fraud controls. Leprechaun also allowed threat actors to alter a victim's banking transactions in real time. For example, when a victim logged into their banking account to transfer money, the threat actors could surreptitiously modify the transaction (including the value and destination) as it was sent from the web browser. This approach circumvents two-factor authentication.

Figure 2. Leprechaun framework. (Source: NSS Labs)

Rock Phish and Avalanche were the first threat groups to perform Automated Clearing House (ACH) fraud, which involves wire transfers from compromised accounts to domestic money mules who forward the money overseas. The threat actors also used the Leprechaun framework for ACH fraud. Targeted financial institutions were unsure how to detect and block fraudulent transfers before a money mule withdrew the funds. However, this type of fraud was easily identifiable after financial institutions established processes and technical controls addressing user-session fraud detection.

Infrastructure disruption

In March 2010, an effort to take down some of Zeus infrastructure impacted Troyak, a bulletproof hosting provider running servers in Kazakhstan, Ukraine, Russia, and Moldova. Troyak was used by Rock Phish, Avalanche, Gozi, and Jabberzeus threat actors. Although the disruption was temporary, it represented the largest number of Zeus servers going offline in one instance. CTU analysis indicates that Andrey Ghinkul, who provided infrastructure to the Rock Phish and Avalanche threat groups, was a key contributor in establishing and operating Troyak.

Operation Trident breACH arrests

In September 2010, law enforcement from the United Kingdom (UK), the Netherlands, Ukraine, and the United States (U.S.) arrested more than 50 individuals suspected of ACH fraud related to Jabberzeus as part of Operation Trident breACH. The U.S. Federal Bureau of Investigation (FBI) noted that the cybercriminals had attempted to steal $220 million and successfully stole $70 million in the U.S. UK law enforcement arrested an additional 19 suspects for fraud. The suspects, led by Ukrainian nationals Yevhen Kulibaba (also known as Jonni) and Yuriy Konovalenko (also known as jtk0), operated the UK division of the cash-out money mule operations for Jabberzeus and potentially other threat groups that used Zeus. Both were sentenced to almost five years in prison.

A U.S. Department of Justice (DoJ) affidavit unsealed in August 2012 named the following Jabberzeus core members. The affidavit also outlines their involvement in ACH fraud and provided probable cause for offenses committed in May 2009.

- Yvacheslav Igorevich Penchukov (also known as tank and father)
- Ivan Viktorvich Klepikov (also known as petr0vich and nowhere)
- Alexey Dmitrievich Bron (also known as thehead)
- Alexey Tikonov (also known as kusanagi)
- Yevhen Kulibaba (also known as jonni)
- Yuriy Konovalenko (also known as jtk0)
- John Doe #1 (also known as lucky12345)
- John Doe #2 (also known as aqua)
- John Doe #3 (also known as mricq)

Zeus resiliency

Following the Operation Trident breACH arrests, computers infected with Jabberzeus were infected with a new Zeus version named Licat (also known as Murofet), suggesting that the threat group continued malicious activities using new malware. This malware was fully functional and ready for deployment before the Jabberzeus members were arrested.

In addition, Spyeye information-stealing malware author Alexander Panin (also known as Harderman and Gribodemon) announced that Bogachev had delivered the Zeus source code and Panin would now support Zeus users and offer a 30% discount on his Spyeye trojan. In January 2011, he released Spyeye version 1.3.05, which merged core Zeus functionality, multiple network backdoors, a credit card number stealer, and web injects. During this period, there were rumors in the criminal underground that Bogachev had not retired from malware development but was “keeping a lower profile” while continuing to work on Zeus versions.

In March 2011, Zeus source code was available for purchase on underground forums, and it was publicly leaked in May 2011. Figure 3 shows Zeus versions created by various threat actors between 2006 and 2013.

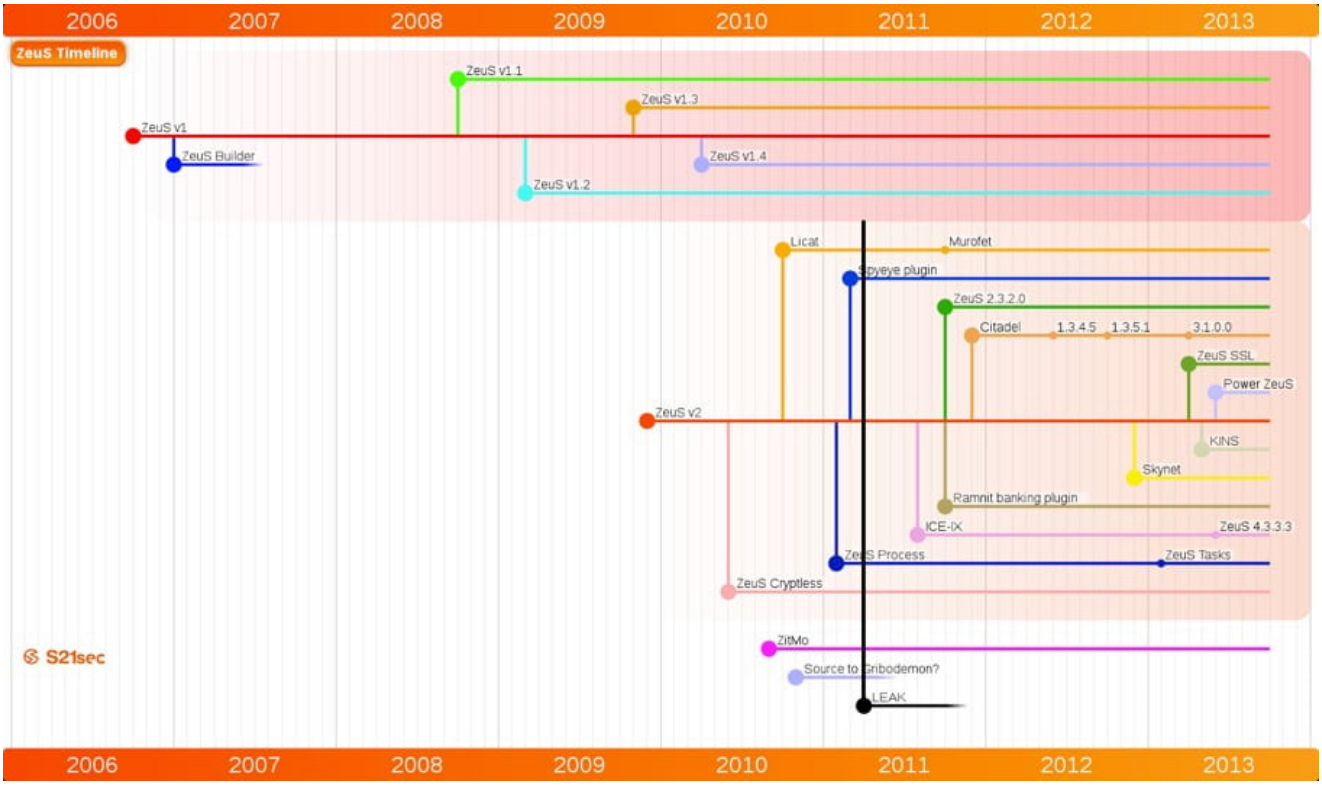


Figure 3. Zeus timeline. (Source: S21)

Gameover Zeus

In September 2011, researchers identified a new Zeus variant named Gameover Zeus (also known as Zeus Game Over, GoZ, and Peer-to-Peer (P2P) Zeus), which added a complex command and control (C2) architecture that used layers of proxies and P2P communication. This new functionality frustrated traditional takedown and attribution activities by law enforcement and security researchers. Gameover Zeus also included an automated transfer system (ATS). Known within the group as "The World Bank Center," this system evolved from the Leprechaun framework used with Jabberzeus. It allowed threat actors to conduct advanced automated transaction alterations, such as checking the account balance and setting maximum amounts to transfer (see Figure 4). These actions were communicated in real time to threat group members.

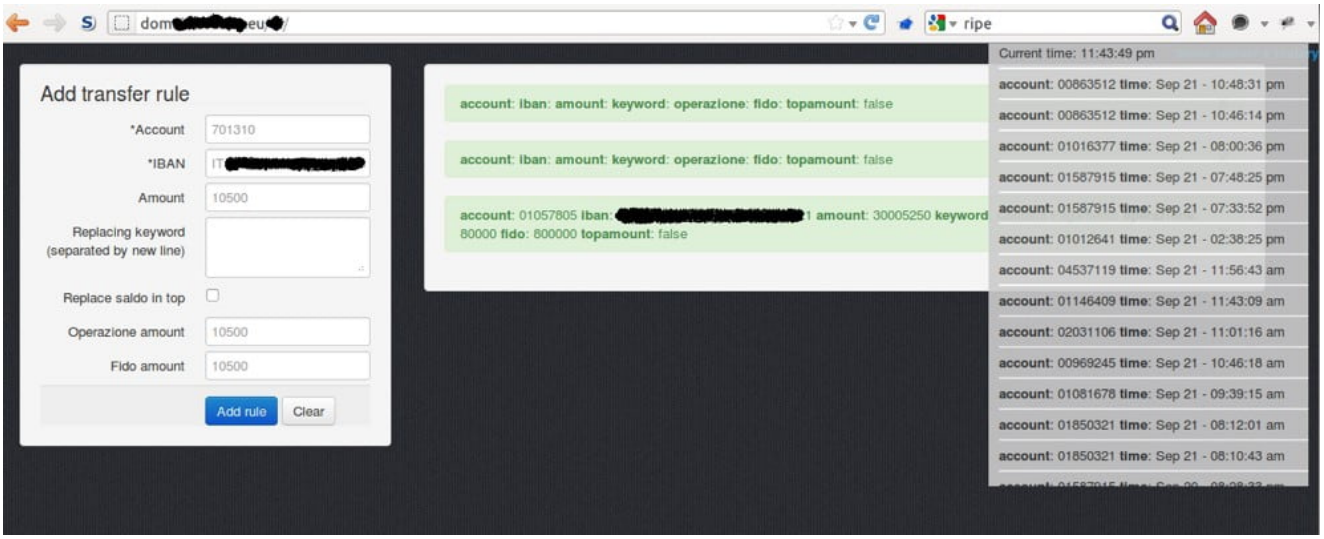


Figure 4. The Gameover Zeus ATS panel. (Source: Minded Security)

Between 2011 and 2014, Gameover Zeus and the ATS module were used to steal several hundred thousand dollars to multimillions in individual ACH transfers and other bank transfer methods. Another common tactic was to access payroll systems and add money mules as payroll recipients. By mid-2014, the Gameover Zeus botnet included approximately one million compromised computers and was responsible for tens of millions of dollars in fraudulent transactions. The Gameover Zeus threat group, which CTU researchers labeled GOLD EVERGREEN, included more than 50 individuals. Bogachev was one of the leaders.

Threat actors could rent a portion of the Gameover Zeus network or its keylogged data store for their criminal enterprises. Renters were required to tithe a portion of the takings to GOLD EVERGREEN. Gameover Zeus was spread by almost every malware distribution method available at the time: spam messages with malicious attachments sent by the Cutwail botnet, Blackhole exploit kit installations, Upatre infections purchased using a pay-per-install (PPI) model, and the Pony Loader malware. The threat actors aimed to install Gameover Zeus on as many computers as possible and had such high confidence in the network's resilience and the bulletproof hosting of its backend infrastructure that it did not attempt to hide the growth and use of this botnet. In 2011, Bogachev created a separate Gameover Zeus network exclusively for espionage. The FBI detected searches for stolen information related to the Ukrainian federal security service, several Georgian government departments, and Turkey's links to Syria.

Gameover Zeus uses several layers of communication to maintain uptime and obfuscate the true location of the final layer of C2 and stolen data collection servers. Its operators also used several bulletproof hosting suppliers. A U.S. government's criminal complaint against GOLD EVERGREEN members alleged that the threat group used Gameover Zeus to download and install the CryptoLocker ransomware. After encrypting victims' computers, the threat actors demanded approximately $750 to decrypt the files.

Operation Tovar

In June 2014, law enforcement and private security companies including SecureWorks participated in Operation Tovar, a coordinated effort to take down the Gameover Zeus botnet. The takedown disrupted Gameover Zeus activity, and despite a re-emergence in July 2014, it never returned to its previous scale.

The DoJ published detailed documents listing the names and nicknames of the GOLD EVERGREEN members. Members Temp Special, DED, and CHINGZ 911 (also known as CHINGZ and MR KYKYPYKY) were listed without real names. The documents name Bogachev as a leader of the threat group and author of Gameover Zeus. The FBI offered a reward of $3 million for information leading to his capture (see Figure 5). As of this publication, Bogachev remains at large and is thought to reside in the Russian Federation. Russian authorities have not publicly arrested Bogachev and have given no indication of that intent.

Figure 5. Bogachev FBI most wanted poster. (Source: FBI)

Dyre and Bugat v5/Dridex

Two weeks after the Gameover Zeus takedown, the Dyre (also known as Dyreza) banking trojan was observed on the Internet. CTU researchers noted a connection between Dyre and the Gozi Neverquest trojan that suggested the same threat actors were responsible for both malware families. Dyre developers and users typically operated during standard working hours: 9 am to 4 pm Monday to Friday (UTC+2 or UTC+3). Reports indicated that some Dyre attacks could be connected to the GOLD EVERGREEN threat group based on the timing, the Upatre downloader, a sophisticated ATS, and the same large-scale cashout methodology.

The Bugat v5 (also known as Dridex) banking trojan, which was observed in July 2014, incorporated a modular architecture and a complex P2P network similar to Gameover Zeus. Bugat v5 is a variant of the Bugat (also known as Cridex) trojan, which CTU researchers identified in 2010. A new threat group named Evil Corporation (also known as EvillCorp) used Bugat v5 as its primary malware to steal credentials and money. Bugat v5 operators also exhibited a standard Monday to Friday working pattern. They primarily targeted financial institutions in Western countries and used the Cutwail spam botnet to send emails containing malicious Office document attachments.

CTU researchers assess that GOLD EVERGREEN diversified its malware portfolio using the Dyre and Bugat v5 trojans to minimize the risks associated with another takedown. In addition to stealing banking credentials, both malware families could be used for espionage. GOLD EVERGREEN used Dyre almost exclusively to steal from large business banking and wealth management accounts, while Bugat v5 was primarily used to steal from retail banking accounts.

Takeover and arrests

In October 2015, CTU researchers worked with the FBI, the UK National Crime Agency (NCA), and the Shadowserver Foundation to take over the Bugat v5 network. On the same day, the DoJ unsealed an indictment announcing that Andrey Ghinkul, who had a history of involvement with infrastructure used by GOLD EVERGREEN, had been arrested in Cyprus and was facing extradition to the United States. Ghinkul was extradited to the U.S. in February 2016 to stand trial in federal court for charges related to administering the Bugat v5 botnets. He pled guilty to charges of conspiracy and damaging a computer and is scheduled to be sentenced on July 13, 2017.

The indictment also described various fraudulent transactions conducted by the Evil Corporation threat group. As of this publication, the Bugat v5 criminal enterprise continues to operate. The NCA arrested 14 suspects in November 2016 and charged them with money mule and laundering offenses. The suspects were linked to thefts of approximately $13.6 million using the Bugat v5 network.

In November 2015, Russian authorities reportedly arrested some GOLD EVERGREEN members operating Dyre, but law enforcement did not announce the arrests until February 2016. Coincidentally, CTU researchers observed Dyre becoming inactive in November.

TrickBot/TheTrick

In October 2016, the TrickBot (also known as TheTrick) information-stealing malware targeted banks in Australia. CTU researchers identified many similarities with Dyre and concluded that TrickBot was derived from Dyre. Between October and early November 2016, the TrickBot threat actors added Canadian, German, and UK banks to their list of targets but have not conducted any fraud as of this publication. Despite the connection to Dyre, there is insufficient information to determine if GOLD EVERGREEN is using TrickBot. It is possible that a copycat threat actor acquired the Dyre source code.

White House sanctions

In late December 2016, the President of the United States issued Executive Order 13964, which sanctioned nine entities responsible for Russian government-based cyberattacks on the U.S. The entities included Russia's Main Intelligence Directorate (Glavnoe Razvedyvatel'noe Upravlenie (GRU)) and Federal Security Service (Federalnaya Sluzhba Bezopasnosti (FSB)), organizations that supported the GRU and FSB, and key staff members. The order also sanctioned Aleksey Alekseyevich Belan (also known as Magg, M4G, and Moy.Yawik) from Riga, Latvia and GOLD EVERGREEN leader Bogachev for "using cyber-enabled means to cause misappropriation of funds and personal identifying information" against U.S. citizens.

Conclusion

This group of tight-knit and loosely connected threat actors has been active for at least 15 years. In spite of multiple indictments and arrests, they continue to represent a major threat to global economies, and appear to be well-versed in the methods and tools used by traditional organized crime groups. CTU researchers conclude that GOLD EVERGREEN is likely operating in a limited capacity as of this publication.

As banks refine their fraud controls and authentication mechanisms, threat groups improve their technical abilities, tools, and targeting capabilities. Threat groups have reduced their focus on retail banking because effective fraud controls defeat a relatively small payout and banks can block a money mule after a single fraudulent transaction. Instead, they are increasingly targeting business banking, share trading, wealth management, superannuation/retirement savings, and payroll systems, where large amounts of money are protected by less sophisticated fraud controls.

CTU researchers recommend that organizations monitor information about active threat groups and their evolving tactics, techniques, and procedures (TTPs), adapting security controls as appropriate. Although persistent threat actors focus on circumventing security

measures, organizations can limit impact by following best practices such as implementing and regularly testing detection and prevention controls, educating users about the risks of spearphishing campaigns and email attachments, and using the principle of least privilege to limit access to sensitive data.