

Adalberto Trujillo

New York University – School of Professional Studies

Cyberspace: Technical, Operational & Strategic Perspectives

Cyber Attack & TIMI Report Assignment

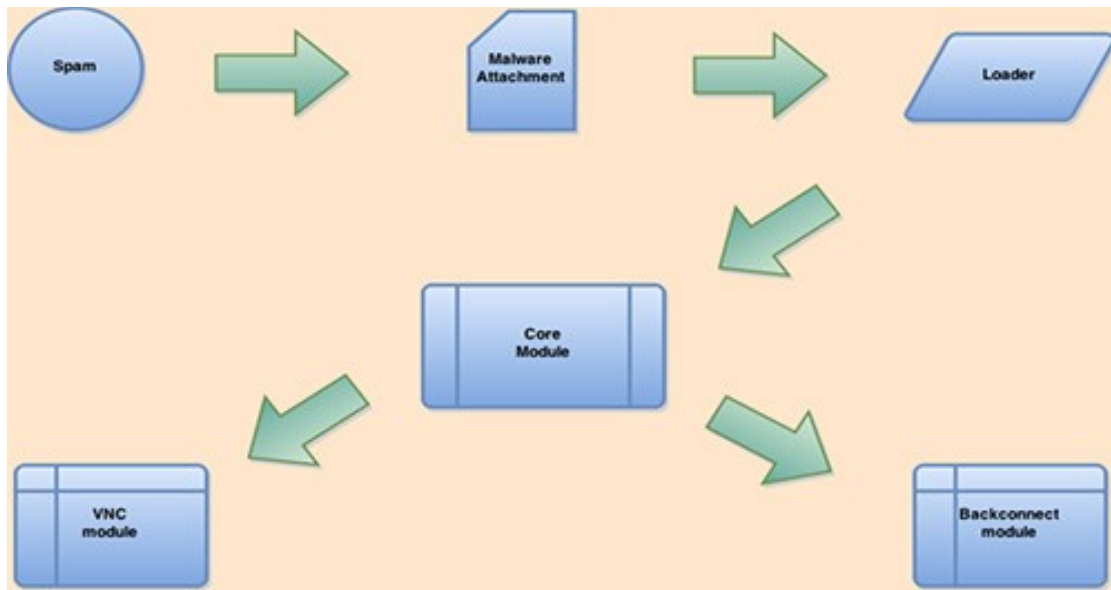
One of the successful attacks that the malicious hacking group Evil Corp used is the Dridex Malware, which was built and successfully exploited to small and large businesses in the United States and abroad in Europe. These attacks were successfully created by the Russian cybercrime-based organization to use it in a sophisticated way. Dridex has existed and first known in the year 2014 and was a “simple bot the authors quickly turned this bot into one of the most sophisticated banking trojans in the morning” (ESET, 2018). Before this malware was considered a serious threat to computer systems, it was built upon the malware called Cidrex. Cidrex is a very sophisticated malware that involves different processes while it is being executed. It not “only infects computers with the purpose of stealing sensitive data from a banking trojan, but it also manages to create email accounts to spam others” (Kovacs, 2012).

Because of how Cidrex was evolving, Evil Corp used this malicious trojan to develop it to make it more complex to work around different places such as browsers, keylogging capabilities, and download additional software. Maksim Yakubets and Igor Turashev have created what is now known as the Dridex Malware, also known as CVE 2017-0199. “The original version of Dridex first appeared in 2012, and by 2015 had become one of the most prevalent financial Trojans. We expect actors using Dridex malware and its derivatives to continue targeting the financial services sector, including both financial institutions and customers” (CISA, 2019). This is what both Yakubets and Turashev did to make it easier to

exploit their targeted users such as small and large businesses individuals in the United States and abroad in Europe.

“Dridex, otherwise known as Bugat and Cridex, was spread far and wide via spam emails” (Brewster). Because of Dridex capabilities to spread easily via phishing emails, Evil Corp included a spear-phishing link or a macros attachment file that contained the Dridex embedded malware once the victim clicks on the link or opens the macro attachment file included in the email. These phishing emails looked legitimate to the victims which fooled the victims into clicking on the link or file attachment included in the email. Once the file or phishing email has been clicked, the malware would execute a connection to an external server to download the actual Dridex malware and perform a silent install in the background which would install a keystroke software and connect to the servers of Evil Corp without any knowledge of the victim.

Not only does it silently installs the Dridex malware and keystroke software but it also installed botnets that were utilized to gather information from the victim and redirected back to the connected external servers of Evil Corp. "The Dridex malware has four primary components: Loader, Core module, VNC module, and the Backconnect module" (Gross, 2015). The loader is the primary bot which is comprised of sub-botnets Each botnet has its own capability of performing actions to the network-connected computer of the victim. Below is an illustrated example of how these bots and sub-botnets worked to perform malicious actions on the victim's networked computer machine.



Source: SecureWorks: <https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation>

Based on the illustrated image above, the phishing email is first sent to the target of choice which can include a macros malicious attachment or a link that has the embedded malware. Once the attachment or click is opened, it will execute a bot that downloads additional bots and malware from an external server that is controlled by the malicious threat actors. The core module serves as the main function for these bots and has the capability of "harvesting credentials, performing man-in-the-browser attacks using web injects" (Gross, 2015). Furthermore, the VNC Module and the Backconnect Module can capture screenshots remotely and sniff through the victim's computer network traffic.

Dridex botnets have been massively distributed to different places around the world. Such places include North America in the United States and Canada, Europe in the UK, Ireland, France Switzerland, Germany, Norway, Austria, Netherlands, Italy, Belgium, Croatia, Bulgaria, and Romania. Furthermore, Dridex botnets were also distributed in the Middle East such as

United Arab Emirates, Qatar, and Israel, in Asia such as Indonesia, Singapore, Malaysia, Hong Kong, China, India, and Vietnam, and in the South Pacific such as Australia and New Zealand.

By looking at the Attack Mitre Workflow Chart, we can determine that collection and command and control were used by Yakubets and Turashev. Below is the graph of the techniques that were used for their email phishing campaign distribution of malware.

Collection 17 techniques	Command and Control 16 techniques
Archive Collected Data (3)	Application Layer Protocol (4)
Audio Capture	Communication Through Removable Media
Automated Collection	Data Encoding (2)
Clipboard Data	Data Obfuscation (3)
Data from Cloud Storage Object	Dynamic Resolution (3)
Data from Configuration Repository (2)	Encrypted Channel (2)
Data from Information Repositories (2)	Fallback Channels
Data from Local System	Ingress Tool Transfer
Data from Network Shared Drive	Multi-Stage Channels
Data from Removable Media	Non-Application Layer Protocol
Data Staged (2)	Non-Standard Port
Email Collection (3)	Protocol Tunneling
Input Capture (4)	Proxy (4)
Man in the Browser	Remote Access Software
Man-in-the-Middle (2)	Traffic Signaling (1)
Screen Capture	Web Service (3)
Video Capture	

Source: <https://attack.mitre.org/#>
1

Main in the browser is “adversary injects

software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user and use the browser as a way to pivot into an authenticated intranet" (MITRE ATT&CK, 2020). Evil Corp was able to collect login information and sessions from their targets especially in financial businesses to steal their login credentials and saving any sessions that will direct the user into financial bank systems. This is one of the tactics that Yakubets and Turashev used to collect sensitive login information to log in to these financial bank systems

Once Yakubets and Turashev collected this login information from these victims, they “used money mules to wire and transfer the stolen money to these malicious threat actors”

(United States Department of Justice, 2019). Money mules were hired to move money around without any kind of suspicion and detection. This is how money transfers were being conducted to profit off from their appointed targets. Unfortunately, Small and large businesses individuals

were fooled by the phishing emails as “74 percent of Dridex spam campaigns used real company names in the sender address and in the email text” (NJCCIC, 2016). By looking at this percentage, it looks like these victim individuals who work for these small and large businesses were tricked into not detecting if the email looked legit or not.

Because of how sophisticated Dridex was created, the phishing emails looked like it came from a legitimate company and legitimate email domain. Proper training policies need to be put in place on how to analyze an email and determine if it’s a phishing email or from a legitimate user. Some of the effects of long-term consequences that can occur if a malicious actor distributes the Dridex malware to a network-connected computer is account access removal. Since this malware distributes bots that each has a certain capability of doing something, such as screen capturing, these malicious actors can obtain bank credentials and change existing passwords to a new one. Furthermore, once access has been gained, these cyber threat actors can manipulate and change information and take full control of it.

Yakubets and Turashev not only stole millions of dollars from small and large businesses companies and organizations around the world but it also damaged their reputation and have a financial impact on these organizations. Some businesses and organizations don’t also report these cyber-attacks which makes it difficult for investigators to prosecute these cybercriminals. Dridex will continue to evolve with further improvements and more additional features that this malware can be capable of doing. Malicious actors will use the same tactics but will get more creative and utilize them for multiple purposes for financial gain, just like Yakubets and Turashev did, in this case.

References:

- “FriedEx: BitPaymer Ransomware the Work of Dridex Authors.” WeLiveSecurity, April 17, 2018. <https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/>.
- Kovacs, Eduard. “Cidrex Trojan Breaks CAPTCHA to Create Yahoo! Email Account.” Softpedia, January 30, 2012. <https://news.softpedia.com/news/Cidrex-Trojan-Breaks-CAPTCHA-to-Create-Yahoo-Email-Account-249437.shtml>.
- “Alert (AA19-339A).” Cybersecurity and Infrastructure Security Agency CISA. Accessed November 12, 2020. <https://us-cert.cisa.gov/ncas/alerts/aa19-339a>.
- Brewster, Thomas. “Cops Knock Down Dridex Malware That Earned 'Evil Corp' Cybercriminals At Least \$50 Million.” Forbes. Forbes Magazine, October 19, 2020. <https://www.forbes.com/sites/thomasbrewster/2015/10/13/dridex-botnet-takedown/?sh=50c815c4415b>.
- Stone-Gross, Brett. “Dridex (Bugat v5) Botnet Takeover Operation.” Secureworks. Accessed November 12, 2020. <https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation>.
- ATT&CK® Navigator. Accessed November 12, 2020. <https://mitre-attack.github.io/attack-navigator/beta/enterprise/>.

- (NPR), Bobby Allyn. "Indictments Against Yakubets and Turashev." DocumentCloud. Accessed November 12, 2020. <https://www.documentcloud.org/documents/6568844-Indictments-Against-Yakubets-and-Turashev.html>.
- "Dridex - NJCCIC Threat Profile." cyber.nj.gov. Accessed November 12, 2020. <https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/dridex>.