Dridex Malware – a Growing Threat to the HPH Sector

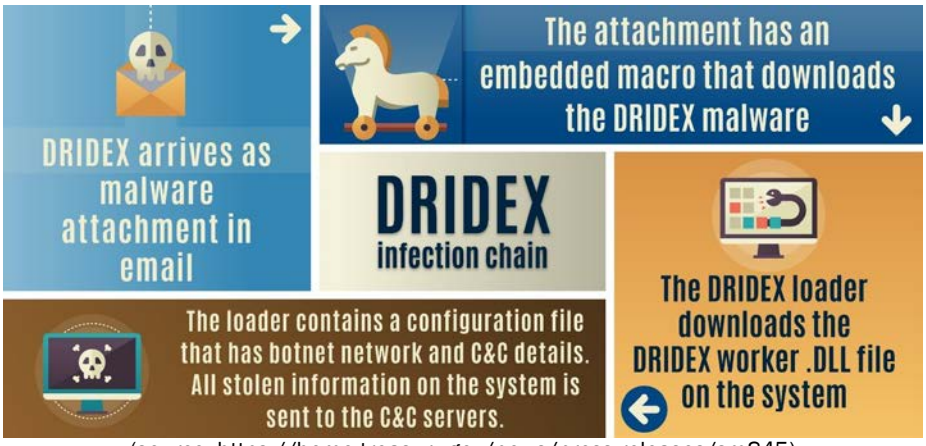
Executive Summary

Dridex was originally developed as a financial Trojan that makes initial contact with its victims via phishing email campaigns and is one of the most prevalent malwares in use today. While Dridex has historically been used in attacks on the financial sector, researchers at ESET determined that the developers of Dridex were also behind the development of the ransomware known as BitPaymer, one of the major forms of ransomware affecting the healthcare and public health (HPH) sector today. Dridex is often used to deliver BitPaymer. A number of recommendations on mitigating Dridex attacks are available in the full report. Dridex malware poses a major risk to the HPH sector.

Report

Version one of Dridex, an evolution of the Bugat/Cridex malware family (circa 2011), was first discovered in 2014. Versions two and three appeared in 2015 and the current version, four, was detected in 2017. Dridex is one of the most prevalent financial Trojans in use today. According to Check Point Software Technologies, a company that inspects over 2.5 billion websites and 500 million files daily, Dridex entered their Threat Index top ten malware families for the first time in March 2020 as number three, and jumped to number one in April 2020.

Dridex was originally developed as a financial Trojan that initially makes contact with its victims via phishing email campaigns. There is usually an attachment with the email that, when opened, launches a hidden or obfuscated macro. It is this macro that then reaches out to an external server to download the actual Dridex malware. In other instances, the macro will launch the Dridex malware, which was previously embedded in the attachment.



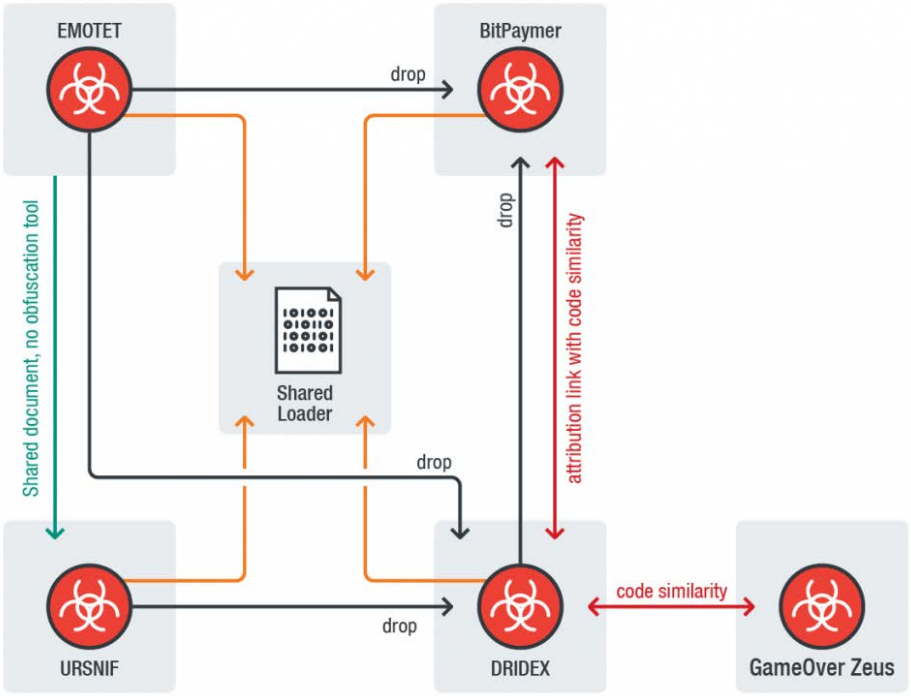
(source: https://home.treasury.gov/news/press-releases/sm845)

Dridex uses a number of different modules depending on the desired effect. As it was developed to target financial activity, it can access browsers, detect interaction with online banking websites, inject keylogging or other software, and steal user login information. It can additionally capture screenshots, add the victim system to a botnet, and download additional malware.

The Russian-based cybercrime organization, Evil Corp, known by various other names such as TA505, SectorJ04, and INDRIK SPIDER, is considered to be the creator of Dridex malware and its main user. It is estimated that Evil Corp has generated over $100 million of profit using Dridex. On December 5, 2019, the U.S. Department of Justice announced charges related to hacking and bank fraud against two Russian nationals, Maksim Yakubets and Igor Turashev, Both are considered to be the developers of Dridex, with Yakubets listed as the leader of Evil Corp. A

reward of up to $5 million is available for information leading to their arrest or conviction.

While Dridex has historically been used in attacks on the financial sector, researchers at ESET determined in early 2018 that the developers of Dridex were also behind the development of the ransomware known as BitPaymer (or FriedEx). BitPaymer is one of the major forms of ransomware affecting the HPH sector and further analysis by Trend Micro reveals a connection between Dridex, BitPaymer, Emotet, and Ursnif malwares. The 2020 Verizon Data Breach Investigations Report reports that within the healthcare sector, 88% of threat actors targeting healthcare are financially motivated, that almost 25% of incidents involve crimeware (ransomware). Overall, across all industries, almost 25% of breaches were as a result of phishing attacks.



(source: https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/)

The U.S. Department of Treasury and Cybersecurity and Infrastructure Security Agency (CISA) recommend the following Dridex mitigations:

- Ensure systems are set by default to prevent execution of macros.
- Inform and educate employees on the appearance of phishing messages, especially those used by the hackers for distribution of malware in the past.
- Update intrusion detection and prevention systems frequently to ensure the latest variants of malware and downloaders are included.
- Conduct regular backup of data, ensuring backups are protected from potential ransomware attack.
- Exercise employees' response to phishing messages and unauthorized intrusion.
- If there is any doubt about message validity, call and confirm the message with the sender using a number or e-mail address already on file.

References

"April 2020's Most Wanted Malware: Agent Tesla Remote Access Trojan Spreading Widely In COVID-19 Related Spam Campaigns," April 2020. https://www.checkpoint.com/press/2020/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/.

"Alert (AA19-339A): Dridex Malware." Cybersecurity and Infrastructure Security Agency CISA, January 2, 2020. https://www.us-cert.gov/ncas/alerts/aa19-339a.

Safran, Magal Baz, and IBM Security's Trusteer. "Dridex's Cold War: Enter AtomBombing." Security Intelligence, March 20, 2020. https://securityintelligence.com/dridexs-cold-war-enter-atombombing/.

"Dridex Malware Kingpin: $5 Million If You Can Find Him," December 13, 2019. https://www.secureworldexpo.com/industry-news/dridex-malware-evil-corp-reward.

Cimpanu, Catalin. "US Charges Two Members of the Dridex Malware Gang | ZDNet," December 5, 2019. https://www.zdnet.com/article/us-charges-two-members-of-the-dridex-malware-gang/.

U.S. Department of the Treasury. "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware." Press Release, June 3, 2020. https://home.treasury.gov/news/press-releases/sm845.

"URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader." TrendLabs Security Intelligence Blog, December 18, 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/.

Poslusny, Michal. "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/.

"2020 Data Breach Investigations Report: Official | Verizon ...," 2020. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.