LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing
Dridex Malware

06/25/2020

Report #: 202006251030

Agenda

- Introduction
- Dridex History
- Dridex Prevalence
- Dridex Technical Details
- Evil Corp
- Bitpaymer Ransomware
- DoppelPaymer Ransomware
- Locky/WastedLocker Ransomware
- Crimeware and the HPH
- Analyst Assessment
- Dridex Mitigations
- Reference Materials
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

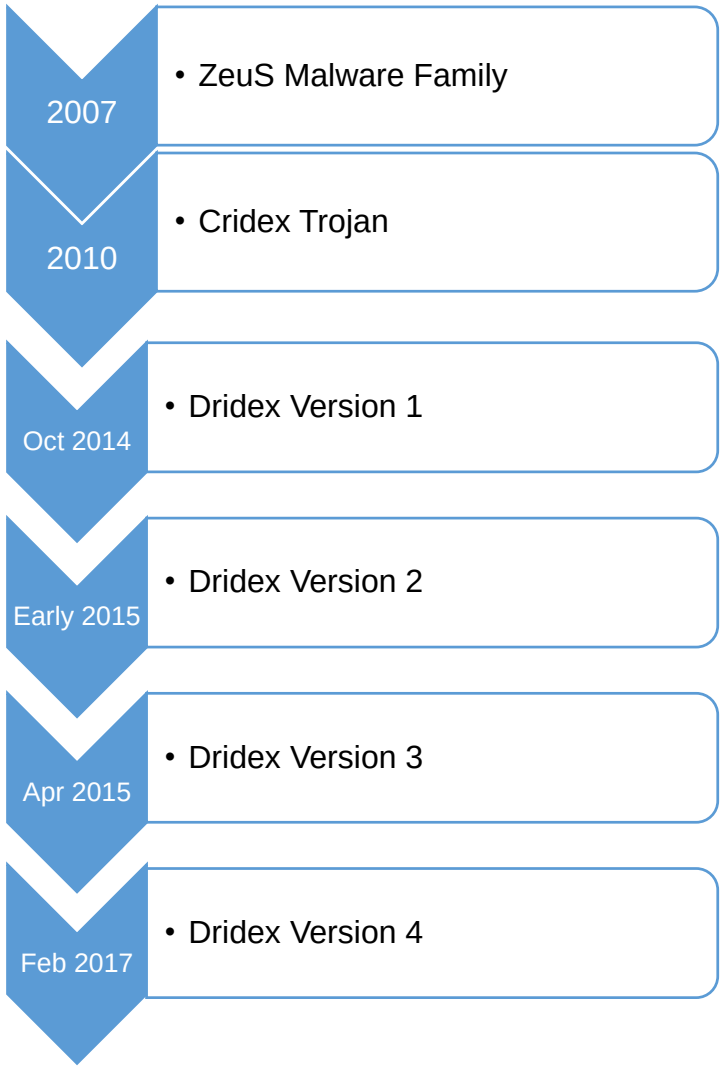
Introduction

- Dridex was originally developed as a financial Trojan that initially makes contact with its victims via phishing/spam email campaigns.
- Dridex is one of the most prevalent malwares in use today.
- While Dridex has historically been used in attacks on the financial sector, researchers have determined that the developers of Dridex were also behind the development of Locky and BitPaymer ransomware, which have affected much of the Healthcare and Public Health (HPH) sector.
- BitPaymer is primarily delivered via Dridex malware, as is DoppelPaymer ransomware, an updated variant of BitPaymer.
- WastedLocker ransomware, first detected last month, was also developed by Evil Corp, and like Locky ransomware is not distributed via Dridex.

Image source: Virus Removal Guidelines

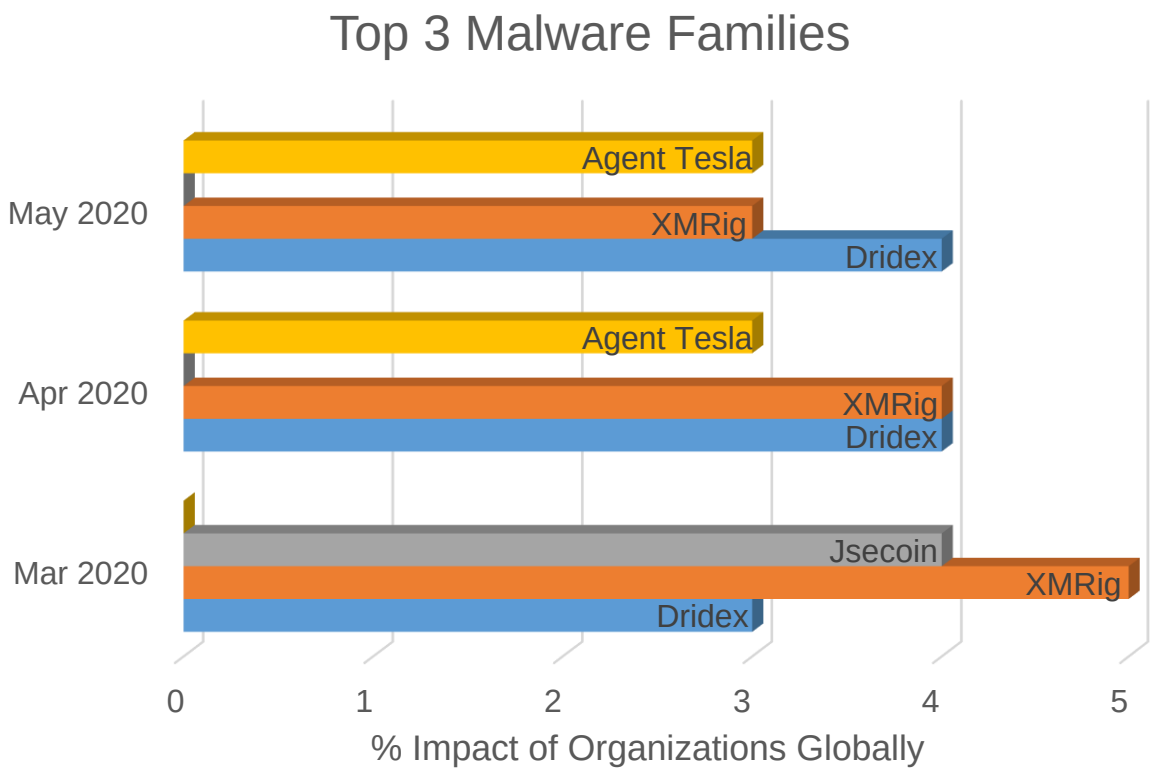
Dridex - History

- 2007 - Birth of the ZeuS malware family
- 2012 - Cridex evolves from GameOver ZeuS
- 2014 - Version one of Dridex, an evolution of the Cridex Trojan, was first discovered in October. Version two followed soon after.
- 2015 - Version two discovered early 2015. Was only active for a few months.
- 2015 - Version three released in April and was the most stable version to date.
- 2017 - Version four, discovered in February, utilizes an injection technique named AtomBombing. The configuration encryption was also upgraded.
- Dridex is one of the most prevalent financial Trojans in use today.



Dridex - Prevalence

- Check Point Software Technologies' Top 3 Malware Families for the last three months.



Dridex - Technical Details

- Dridex was originally developed as a financial Trojan that initially makes contact with its victims via phishing/spam 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.

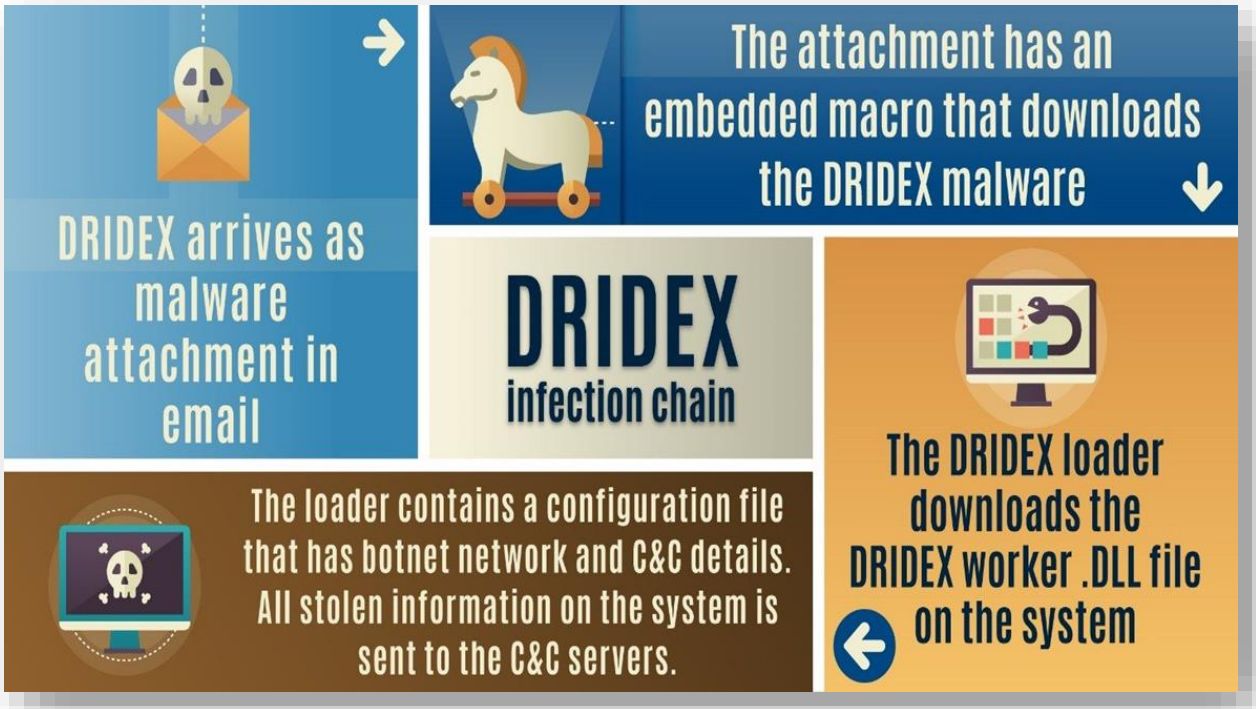


Image source: Treasury Department

Dridex - Technical Details (cont.)

- 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
  - steal user login information
- It can additionally
  - capture screenshots
  - add the victim system to a botnet
  - download additional malware

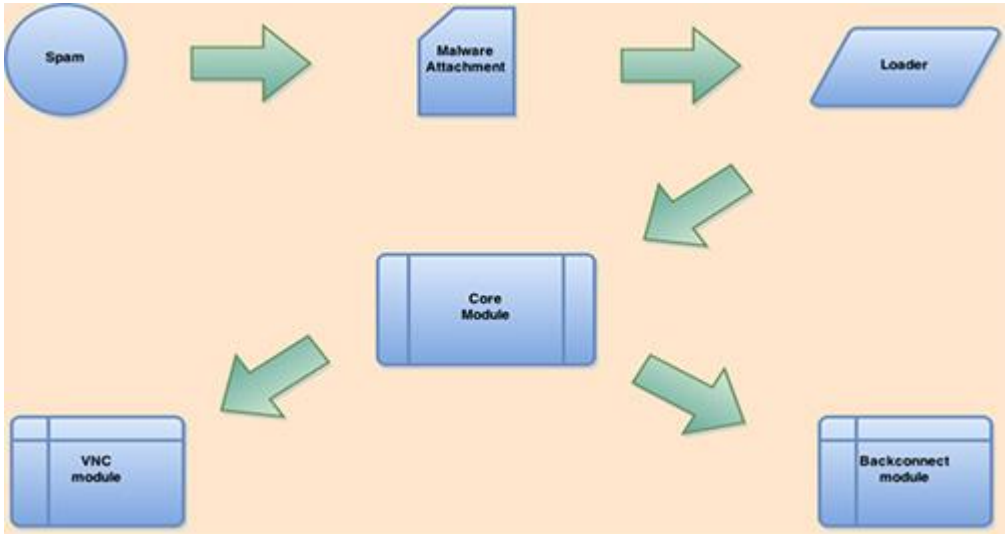


Image source: Secure Works

Dridex - Technical Details (cont.)

- Version four of Dridex, which appeared in February 2017, uses the AtomBombing technique.
- This technique was only discovered by researchers from enSilo in October 2016.
- It allows malware to inject code without making the usual API calls used with code injection:
  - VirtualAllocEx, to allocate a buffer in the remote process with RWX permissions;
  - WriteProcessMemory, to copy the payload to the allocated buffer
  - CreateRemoteThread, to execute the payload
- Instead, AtomBombing uses Window's atom tables. Applications store strings in the tables and receives an "atom", that can be used to access the string.
- AtomBombing uses the atom tables along with different APIs to inject the code, which is much more difficult for common security tools to detect.

Image source: Bigstock

Dridex - Technical Details (cont.)

Domain	ID	Name	Use
Enterprise	T1071	Application Layer Protocol: Web Protocols	Dridex has used HTTPS for C2 communications.
Enterprise	T1573	Encrypted Channel: Symmetric Cryptography	Dridex has encrypted traffic with RC4.
Enterprise	T1573	Encrypted Channel: Asymmetric Cryptography	Dridex has encrypted traffic with RSA.
Enterprise	T1185	Man in the Browser	Dridex can perform browser attacks via web injects to steal information such as credentials, certificates, and cookies.
Enterprise	T1090	Proxy	Dridex contains a backconnect module for tunneling network traffic through a victim's computer. Infected computers become part of a P2P botnet that can relay C2 traffic to other infected peers.
Enterprise	T1219	Remote Access Software	Dridex contains a module for VNC.

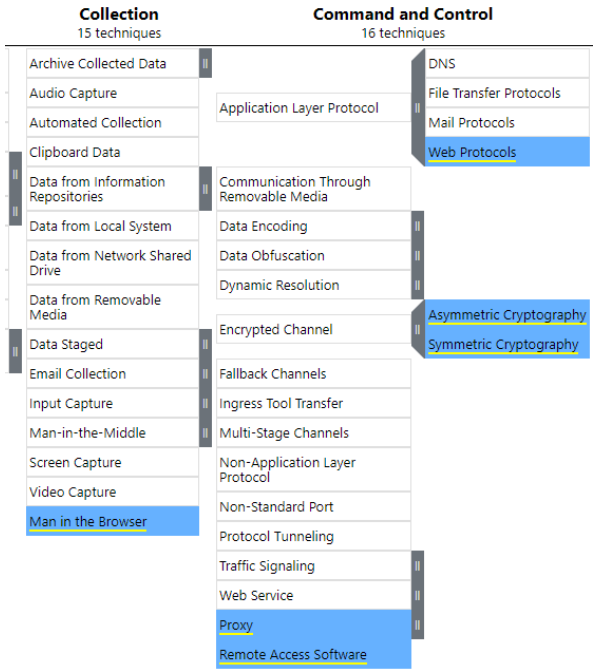


Image source: MITRE

Evil Corp

- The Russian-based cybercrime organization, self-named as Evil Corp, is considered to be the creator of Dridex malware and its main user.
- Evil Corp is also known by various other names in the threat intelligence community such as:
  - TA505
  - SectorJ04
  - INDRIK SPIDER
  - GRACEFUL SPIDER
  - GOLD TAHOE
  - Dudear
- It is estimated that Evil Corp has generated over $100 million of profit using Dridex.

Image source: Cloud City 7

Evil Corp

- On December 5, 2019, the US 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.

Image source: Department of Justice

Image source: FBI

Bitpaymer Ransomware

- Dridex has historically been used in attacks on the financial sector.
- BitPaymer (also known as FriedEx) ransomware was first identified in August 2017.
- In 2018, researchers at ESET determined that the developers of Dridex also developed BitPaymer.
- BitPaymer is one of the major forms of ransomware affecting the HPH sector.
- Further analysis by Trend Micro reveals a connection between Dridex, BitPaymer, Emotet, and Ursnif malwares.

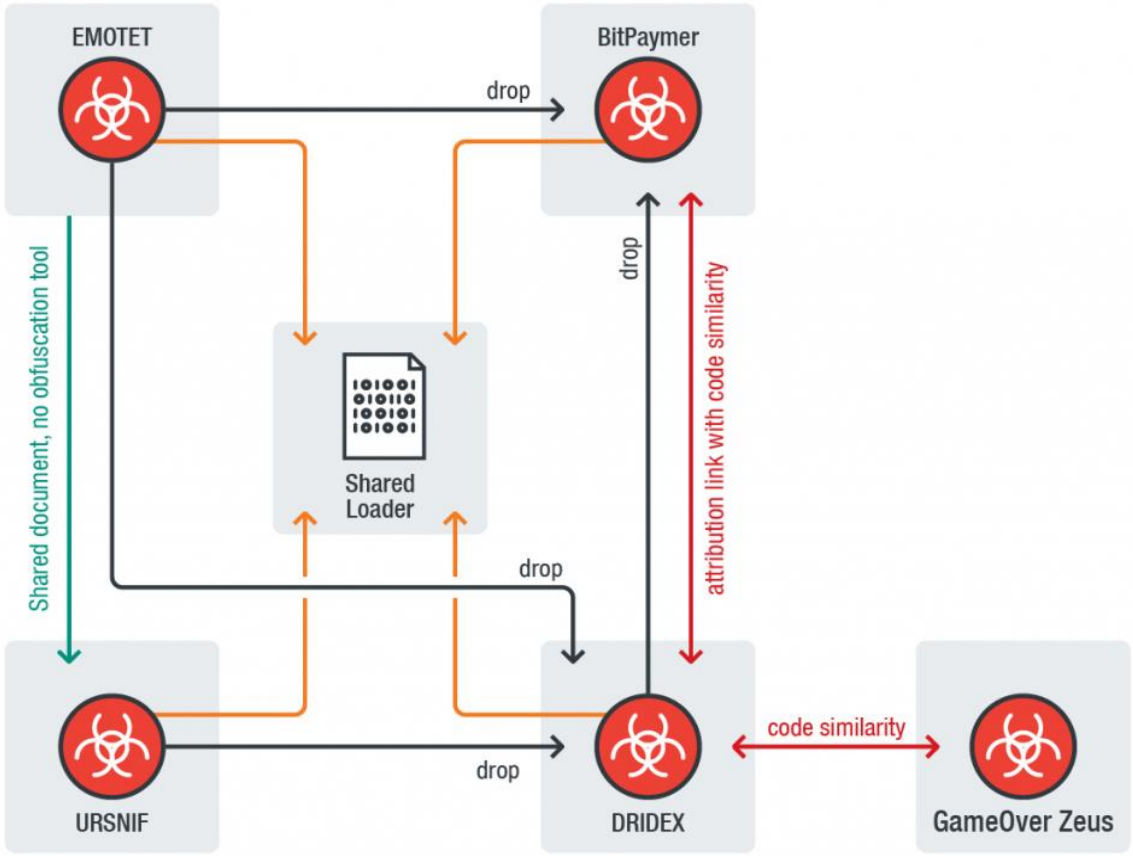
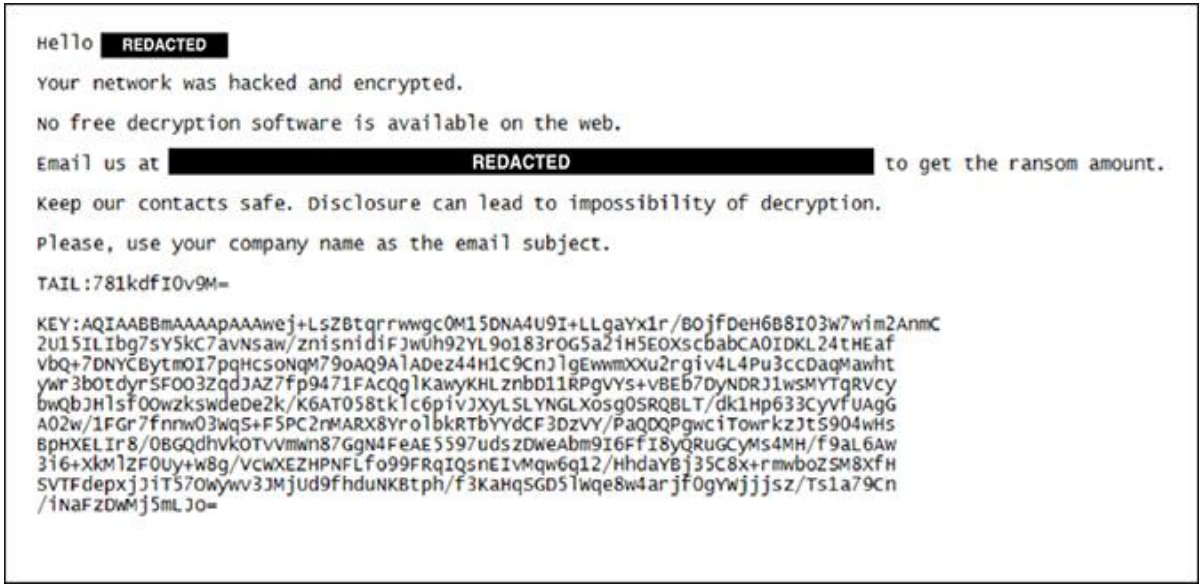


Image source: Trend Micro

Bitpaymer Ransomware (cont.)

- The first BitPaymer ransom note contained the ransom demand and a URL for a TOR-based portal for payment.
- After the first month of operation, the ransom amount was removed from the note, and the payment portal was removed in July 2018.
- Since then, the ransom note only contains two contact emails.
- In November 2018, the BitPaymer ransom note was updated to include the victim's name.



Hello [REDACTED]

Your network was hacked and encrypted.

No free decryption software is available on the web.

Email us at [REDACTED] to get the ransom amount.

Keep our contacts safe. Disclosure can lead to impossibility of decryption.

Please, use your company name as the email subject.

TAIL:781kdfI0v9M=

KEY:AQIAABBmAAAApAAAwej+LsZBtqrrwwgc0M15DNA4U9I+LLgaYx1r/BOjfDeH6B8I03W7wim2AnmC
2U15ILIbg7sY5kC7avNsaw/znisnidiFJwUh92YL9o183rOG5a2iH5EOXscbabCAOIDKL24tHEaf
VbQ+7DNYCBytmOI7pqHcsoNqM79oAQ9AlADez44H1C9CnJlgEwwmXXu2rgiv4L4Pu3ccDaqMawht
yWr3bOtdyrSFOO3ZqdJAZ7fp9471FAcQglKawyKHLznbD11RPgVYs+vBEb7DyNDRJ1wsMYTqRVcy
bwQbJHlsfOOwzkswdeDe2k/K6AT058tklc6pivJXyLSLYNGLXosgOSRQBLT/dk1Hp633CyVfUAgG
A02w/1FGr7fnnw03WqS+F5PC2nMARX8YrolbkRTbYYdCF3DzVY/PaQDQPgwciTowrkzJtS904wHs
BpHXELIr8/OBGQdhVkOTvvmwn87GgN4FeAE5597udszDWeAbm9I6FfI8yQRuGCyMs4MH/f9aL6Aw
3i6+XkMlZF0Uy+W8g/VCWXEZHPNFLfo99FRqIQsnEIvMqw6q12/HhdaYBj35C8x+rmwboZSM8XfH
SVTFdepxjJiT57Owywv3JMjud9fhduNKBtph/f3KaHqSGD5lWqe8w4arjf0gYwjjjsz/Ts1a79Cn
/iNaFZDWMj5mLJo=

Image source: CrowdStrike

DoppelPaymer Ransomware

- DoppelPaymer ransomware, first seen in the wild in mid-2019 by CrowdStrike Intelligence, shares significant amounts of code with BitPaymer.
- However, CrowdStrike analysts believe that the differences between the two ransomwares may indicate that one or more members of Evil Corp have left the group, using code from both Dridex and BitPaymer to form DoppelPaymer.
- The DoppelPaymer ransom note is almost identical to the BitPaymer ransom note.
- There are encryption differences between the malwares and DoppelPaymer has added ProcessHacker to terminate processes that interfere with file encryption.

Image source: How To Fix Guide

Locky/WastedLocker Ransomware

- Locky Ransomware
  - Detected in February 2016. Launched major US campaign in August and went quiet in December.
  - Returned in January 2017. Launched second major US campaign in August and went quiet again as BitPaymer ransomware was launching.
- WastedLocker Ransomware
  - Detected in May 2020 and does not have much in common with BitPaymer.
  - Distributed by the SocGholish fake update framework versus Dridex.

Image source: SecNews

Cybercrime and the HPH

- The 2020 Verizon Data Breach Investigations Report reports that overall, across all industries :
  - Almost 25 percent of breaches were as a result of phishing attacks
  - 27 percent were ransomware

- Within the HPH:
  - 88 percent of threat actors targeting healthcare are financially motivated
  - Almost 25 percent of incidents involve crimeware

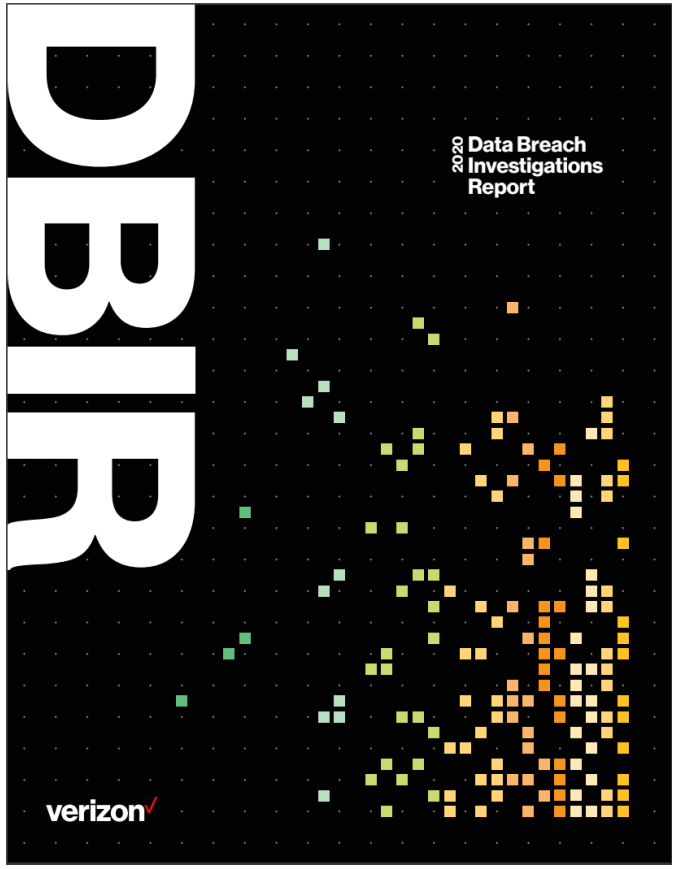


Image source: Verizon

Analyst Assessment

- ***HC3 analysts assess with high confidence that Dridex malware poses a major risk to the Healthcare and Public Health (HPH) sector.***
- The historical success of Dridex, combined with it currently being one of the most active malware families, increases its risk in general.
- Its association with BitPaymer and DoppelPaymer ransomware, and the fact that 25 percent of healthcare industry breaches involve crimeware, makes it a particular risk to the healthcare industry.

Image source: VectorStock

Dridex Mitigations

- Department of Treasury and Cybersecurity and Infrastructure Security Agency (CISA) recommend the following Dridex-specific mitigations:

  - Ensuring 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.

Image source: Wikipedia

Image source: Wikipedia

Reference Materials

References

- US-CERT Alert (AA19-339A)
  - https://www.us-cert.gov/ncas/alerts/aa19-339a
- March 2020's Most Wanted Malware: Dridex Banking Trojan Ranks On Top Malware List For First Time
  - https://www.checkpoint.com/press/2020/march-2020s-most-wanted-malware-dridex-banking-trojan-ranks-on-top-malware-list-for-first-time/
- April 2020's Most Wanted Malware: Agent Tesla Remote Access Trojan Spreading Widely In COVID-19 Related Spam Campaigns
  - https://www.checkpoint.com/press/2020/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/
- May 2020's Most Wanted Malware: Ursnif Banking Trojan Ranks on Top 10 Malware List for First Time, Over Doubling Its Impact on Organizations
  - https://www.checkpoint.com/press/2020/may-2020s-most-wanted-malware-ursnif-banking-trojan-ranks-on-top-10-malware-list-for-first-time-over-doubling-its-impact-on-organizations/
- Dridex's Cold War: Enter AtomBombing
  - https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
- Dridex Malware Kingpin: $5 Million if You Can Find Him
  - https://www.secureworldexpo.com/industry-news/dridex-malware-evil-corp-reward
- US charges two members of the Dridex malware gang
  - https://www.zdnet.com/article/us-charges-two-members-of-the-dridex-malware-gang/

References

- Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware
  - https://home.treasury.gov/news/press-releases/sm845
- URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader
  - https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
- FriedEx: BitPaymer ransomware the work of Dridex authors
  - https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/
- Verizon 2020 Data Breach Investigations Report (DBIR)
  - https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
- Mitre ATT&CK® Navigator - Dridex
  - https://attack.mitre.org/beta/software/S0384/
- Mitre ATT&CK® Software - Dridex
  - https://mitre-attack.github.io/attack-navigator/beta/enterprise/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fbeta%2Fsoftware%2FS0384%2FS0384-enterprise-layer.json
- BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0
  - https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/#:~:text=CrowdStrike%C2%AE%20Intelligence%20has%20identified,variant%20identifying%20itself%20as%20BitPaymer.&text=We%20have%20dubbed%20this%20new,ransomware%20operated%20by%20INDRIK%20SPIDER.

References

- Dridex Banking Trojan Distributed Through Word Documents
  - https://unit42.paloaltonetworks.com/dridex-banking-trojan-distributed-word-documents/
- Dridex (Bugat v5) Botnet Takeover Operation
  - https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation
- WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group
  - https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
- Locky Ransomware
  - https://www.knowbe4.com/locky-ransomware
- The return of Locky: a closer look at 2017's largest malware campaign
  - https://www.itgovernance.co.uk/blog/the-return-of-locky-a-closer-look-at-2017s-largest-malware-campaign#:~:text=The%20return%20of%20Locky%3A%20a%20closer%20look%20at%202017's%20largest%20malware%20campaign,-Camden%20Woollven%2022nd&text=The%20resurgence%20of%20Locky%20ransomware,hours%20on%2028%20August%202017.

Questions

Questions

Upcoming Briefs

- No meeting (7/2)
- Business Email Compromise (BEC) (7/9)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV