Pony/Fareit Malware: A Growing Threat to the Healthcare and Public Health Sector

Executive Summary

Pony malware, also known as Fareit, is a growing threat to the Healthcare and Public Health (HPH) sector. Classified by Trend Micro as a Trojan-Spyware, this crimeware is primarily used to steal user and File Transfer Protocol (FTP) credentials and passwords, download other payloads, and bring compromised systems into a botnet. It is one of the most widely used information stealers in action today. Pony is commonly associated with CVE-2017-11882, which according to a recent FBI/CISA report, is in the top 10 list of most exploited vulnerabilities from 2016 to 2019, and is also one of the top three vulnerabilities exploited by nation state actors. Pony/Fareit malware poses a great risk to the HPH sector; it is used in one of the most exploited vulnerabilities (CVE-2017-11882), employs the capabilities used in 80% of all breaches involved with hacking, and functions as both a credential harvester and downloader, making it one of the more versatile existing malwares.

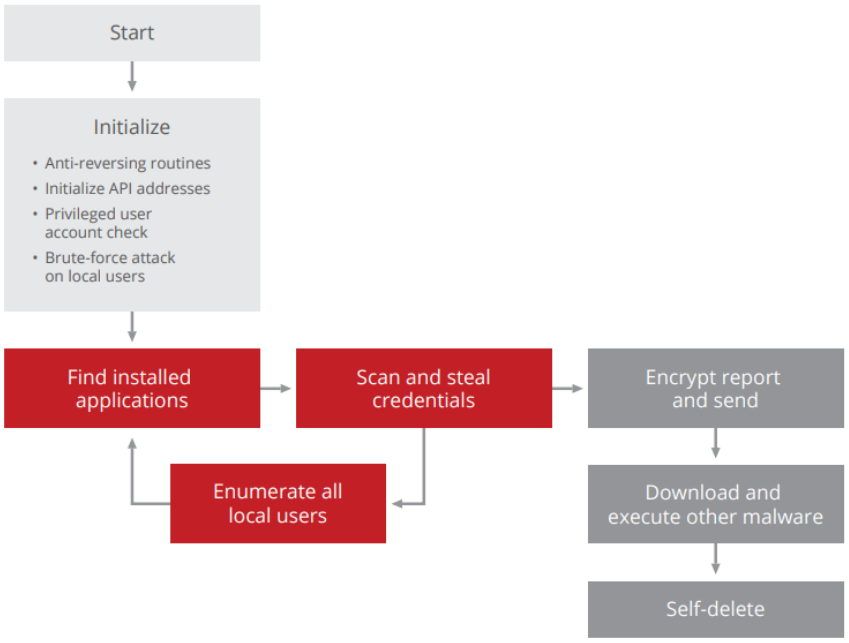
Report

Pony is commonly associated with CVE-2017-11882, which according to a recent FBI/CISA report, is in the top 10 list of most exploited vulnerabilities from 2016 to 2019, and is also one of the top three vulnerabilities exploited by nation state actors. The 2020 Verizon Data Breach Investigations Report states that "over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials," which is Pony/Fareit's specialty. Additionally, 88% of healthcare breaches are financially motivated, making the HPH sector a prime target for crimeware-based attacks.

Pony malware's usage and capabilities have grown since it was first exposed by malware researchers in 2011. The source code for version 1.9 was leaked in December 2012 and version 2.0 was leaked in January 2015. The latest known existing version is 2.2; since its initial creation, Pony malware's antivirus detection capabilities have improved, including anti-disassembly, anti-emulation, and packing. In addition, crypto-currency wallet theft capabilities have been added, and the number of applications from which Pony malware can steal credentials has increased.

The malware is broken down into three parts: Pony Builder, Pony Bot, and a server-side control panel. The Pony Builder is used to create the Pony Bot, or client, that is downloaded to the targeted systems. The control panel allows the attacker to manage and view any information returned by the Bot. Common infection vectors include spam and phishing campaigns, DNS poisoning, and exploit kits.

The execution flow of Pony/Fareit malware is as follows:



Experts recommend the following actions (among others) to avoid infection by malware such as Pony:

- Utilize multifactor authentication
- Create strong passwords and change them frequently
- Use different passwords for every account or service
- Ensure awareness of the latest phishing techniques
- Disable Microsoft (MS) Office macros by default
- Avoid enabling MS Office macros in attachments
- Take extra care when opening email attachments
- Install/update security software on all system

Verizon recommends implementing the following Center for Internet Studies (CIS) Critical Security Controls (CSC):

- CSC 12 – Boundary Defense
- CSC 13 – Data Protection
- CSC 17 – Implement a Security Awareness Training Program

References

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

"CISA, FBI Breakdown Most Exploited Vulnerabilities." Digital Guardian, May 13, 2020. https://digitalguardian.com/blog/cisa-fbi-breakdown-most-exploited-vulnerabilities.

"Emerging Threat on FAREIT Resurgence," April 13, 2020. https://success.trendmicro.com/solution/1118407-emerging-threat-on-fareit-resurgence.

"McAfee Labs Threats Reports June 2017 – Threat Research | McAfee," June 2017. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf.

"Pony: Malware Trends Tracker." Pony | Malware Trends Tracker, May 28, 2020. https://any.run/malware-trends/pony.

"Spoofed Healthcare Malspam Campaign Delivers Hancitor ...," n.d. https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-humana-healthcare.pdf.

Journal, HIPAA. "Healthcare Cybersecurity." HIPAA Clicks, June 3, 2020. https://hipaaclicks.com/category/healthcare-cybersecurity/.

Lake, Josh. "Pony: A Breakdown of the Most Popular Malware in Credential Theft." Acunetix, September 25, 2018. https://www.acunetix.com/blog/articles/pony-malware-credential-theft/.