“LokiBot,” the malware that steals your most sensitive data, is on the rise

reader comments

18 with 18 posters participating

Share this story

Federal and state officials are seeing a big uptick in infections coming from LokiBot, an open source DIY malware package for Windows that’s openly sold or traded for free in underground forums. It steals passwords and cryptocurrency wallets, and it can also download and install new malware.

In an alert published on Tuesday, the Department of Homeland Security’s Cybersecurity and Infrastructure Agency and the Multi-State Information Sharing & Analysis Center said LokiBot activity has scaled up dramatically in the past two months.

The increase was measured by “EINSTEIN,” an automated intrusion-detection system for collecting, correlating, analyzing, and sharing computer security information across the federal civilian departments and agencies.

“CISA has observed a notable increase in the use of LokiBot malware by malicious cyber actors since July 2020,” Tuesday’s alert stated. “Throughout this period, CISA’s EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected persistent malicious LokiBot activity.”

While not quite as prevalent or noxious as the Emotet malware, LokiBot remains a serious and widespread menace. The infostealer spreads through a variety of methods, including malicious email attachments, exploitation of software vulnerabilities, and trojans sneaked into pirated or free apps. Its simple interface and reliable codebase make it attractive to a wide range of crooks, including those who are new to cybercrime and have few technical skills.

EINSTEIN isn’t the only source that’s measuring an increase in LokiBot activity of late. Sherrod DeGrippo, senior director of threat research and detection at security firm ProofPoint, said Emotet typically dwarfs LokiBot by an order of magnitude, with volume on Monday being about 300,000 for the former versus 1,000 for the latter. More recently, there have been exceptions. Last Thursday, for instance, DeGrippo counted a LokiBot run of more than 1 million messages.

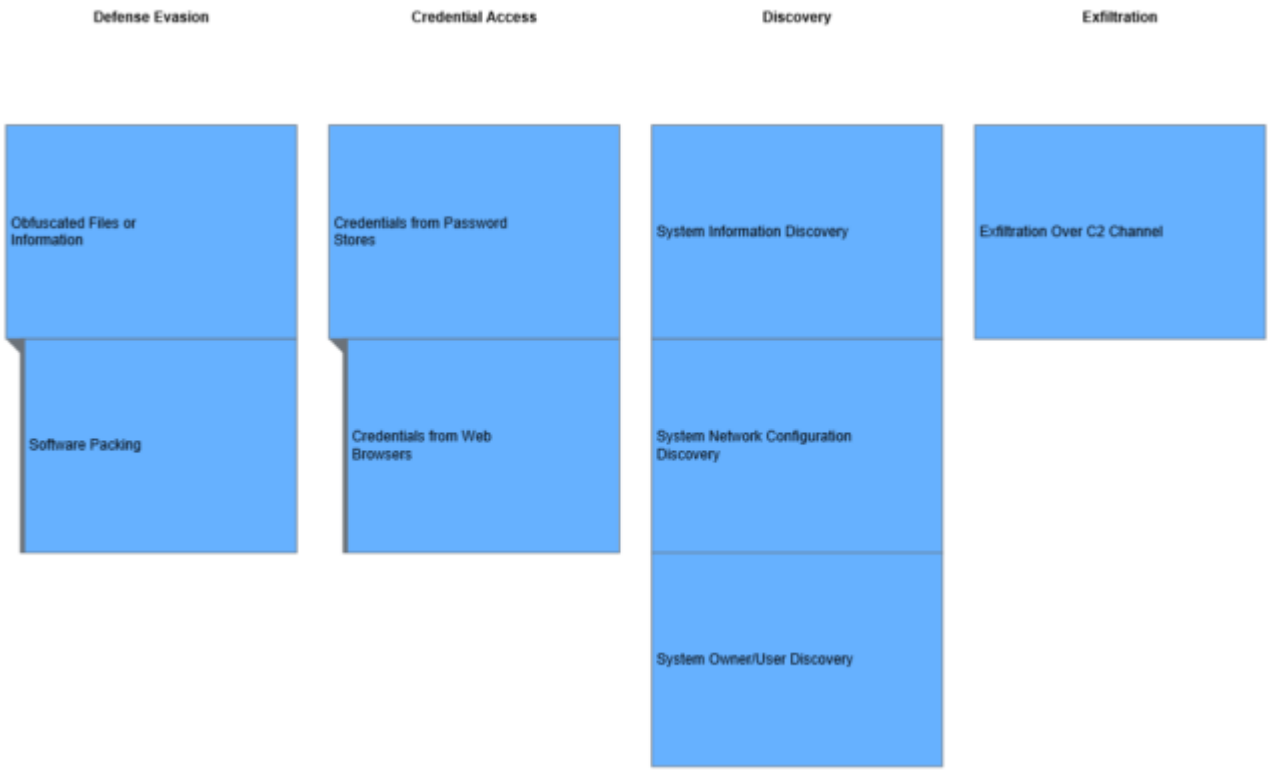
Full-featured

The malware includes a keylogger that records passwords and other sensitive keystrokes, code that harvests passwords stored in browsers, administrative tools, and cryptocurrency wallets, and can steal information from more than 100 different applications, according to security firm Gigamon.

According to the MITRE ATT&CK knowledge base of adversary tactics and techniques, a fuller list of capabilities and features includes:

- Discover the domain name of the infected host.
- Use obfuscated strings with base64 encoding.
- Several packing methods for obfuscation of binary files.
- Ability to discover the username on the infected host.
- Ability to initiate contact with command and control to exfiltrate stolen data.
- Process hollowing to inject into legitimate Windows process vbc.exe.
- The ability to capture input on the compromised host via keylogging.
- Use of HTTP for command and control.
- The ability to discover the computer name and Windows product name/version.
- Can be executed through malicious documents contained in spear-phishing emails.
- Can steal credentials from multiple applications and data sources including Windows operating system credentials, email clients, FTP, and Secure File Transfer Protocol clients.
- The ability to steal credentials from multiple applications and data sources including Safari and Chromium and Mozilla Firefox-based Web browsers.
- The ability to copy itself to a hidden file and directory.

The graphic below, also from the MITRE ATT&CK, lays out some of its capabilities in targeting enterprises.



MITRE ATT&CK

Researchers at Palo Alto Networks said that the LokiBot is the most popular tool used by SilverTerrier, a Nigerian crime group known for performing business-email compromises that scam high-ranking employees into wiring company funds overseas.

Protecting against LokiBot involves the usual advice about being highly judicious before opening email attachments, not enabling Microsoft Office macros without ample experience and a good reason, steering clear of software that’s pirated or comes from unknown sources, and remaining skeptical online.

https://arstechnica.com/?p=1708765