

SmokeLoader Malware Used to Augment Amadey Infostealer

blogs.blackberry.com/en/2022/07/smokeloader-malware-used-to-augment-amadey-infostealer

The BlackBerry Research & Intelligence Team



Amadey has updated its infection methods, and now employs SmokeLoader to get onto victims' systems. In past iterations, this information stealer has used exploit kits such as RigEK and Fallout EK to gain access to vulnerable machines.

Amadey is a criminal-to-criminal (C2C) botnet infostealer project, meaning it is a service made available on the black market by criminals, for purchase by other criminals. It was first discovered in 2018, and highlighted by the BlackBerry Threat Research Team in 2020. While it is primarily used for collecting information about a victim's computing environment, it can also be used to deliver additional malicious modules.

Recently, Amadey has been observed using SmokeLoader loader malware to spread a new and highly aggressive Amadey Bot variant. Threat actors have concealed the loader in "cracked" software and keygen (key generator) sites, which offer the lure of providing illicit free access to licensed software. The SmokeLoader family has been actively relying on this scheme for transmission since at least the beginning of this year.

Amadey Information Stealing Methods

After Amadey completes its initial setup processes, it connects to a remote, attacker-controlled command-and-control (C2) server. It then downloads a plugin to collect system, application, and antivirus (AV) information from the victim's machine. This information allows the threat actor to identify both sensitive information for exfiltration as well as details of any antivirus tools on the system, so they can be evaded.

This recent version of the infostealer includes enhanced features compared to its predecessor. These include:

- Scheduled tasks for persistence
- Advanced reconnaissance options
- User account control (UAC) bypassing
- Tailored defense evasion strategies

After attackers have successfully breached a system, they then have the opportunity to install additional malicious components.

Amadey and SmokeLoader Connection

The BlackBerry Threat Research Team has observed SmokeLoader being hidden in cracks and keygens for several brands of popular software applications. The threat actor behind it has been relying on black SEO to seed malicious results to get prime placement at the top of search engine results, so those seeking cracks can easily find these Trojanized files to download and run.

Since it's publicly known that some AV vendors may block cracks and keygens, some people explicitly disable their endpoint security products before downloading these files, or they ignore detection alerts and proceed with the download. So even if the sample is widely detected, there is room for a successful infection, due to the victim specifically allowing it.

SmokeLoader has been very active of late. According to telemetry monitored by BlackBerry, most targets are in the United States, followed by Japan, Mexico, and Brazil. Over 25,000 different SmokeLoader samples have been observed in our telemetry during the past three months.

It's notable that a quarter of all attempts to infect have hit targets in the healthcare industry.

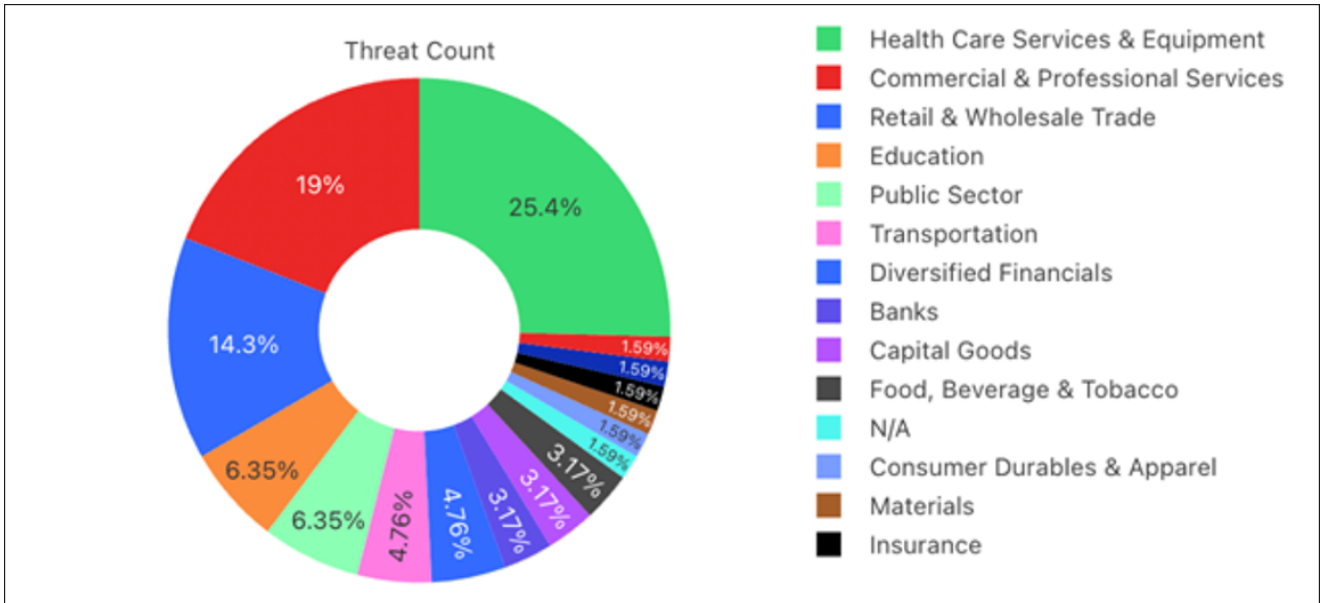


Figure 1 – “Industries most targeted by SmokeLoader worldwide”

BlackBerry Stops SmokeLoader and Amadey


Customers using CylancePROTECT® are protected from SmokeLoader and Amadey augmented by SmokeLoader.

To combat this highly effective and infectious malware variant, BlackBerry recommends using artificial intelligence-based agents trained for threat detection on millions of both safe and unsafe files. For example, BlackBerry’s Cylance® AI uses automated security agents to block Amadey based on numerous file attributes and malicious behaviors, rather than relying on a specific file signature.


About CylancePROTECT

CylancePROTECT is an endpoint protection platform (EPP) from BlackBerry that employs Cylance AI’s advanced, seventh-generation, machine learning models to provide a predictive advantage against both zero-day threats and legacy cyberattacks.

Related Reading


BlackBerry
 Intelligent Security. Everywhere.

THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.
BlackBerry.com/beacon


FINDING BEACONS



About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.
