FIN7 Backdoor Masquerades as Ethical Hacking Tool

By Tara Seals

Published: 2021-05-14 · Archived: 2026-04-05 13:41:22 UTC

The financially motivated cybercrime gang behind the Carbanak RAT is back with the Lizar malware, which can harvest all kinds of info from Windows machines.

The notorious FIN7 cybercrime gang, a financially motivated group, is spreading a backdoor called Lizar under the guise of being a Windows pen-testing tool for ethical hackers.

According to the BI.ZONE Cyber Threats Research Team, FIN7 is pretending to be a legitimate organization that hawks a security-analysis tool. They go to great lengths for verisimilitude, researchers said: “These groups hire employees who are not even aware that they are working with real malware or that their employer is a real criminal group.”

Since 2015, FIN7 has targeted point-of-sale systems at casual-dining restaurants, casinos and hotels. The group typically uses malware-laced phishing attacks against victims in hopes they will be able to infiltrate systems to steal bank-card data and sell it. Since 2020, it has also added ransomware/data exfiltration attacks to its mix, carefully selecting targets according to revenue using the ZoomInfo service, researchers noted.

Its choice of malware is always evolving, including occasionally using never-before-seen samples that surprise researchers. But its go-to toolkit has been Carbanak remote-access trojan (RAT), which previous analysis shows is highly complex and sophisticated compared with its peers: It’s basically a Cadillac in a sea of golf carts. Carbanak is typically used for reconnaissance and establishing a foothold on networks.

Lately, though, BI.ZONE researchers have noticed the group using a new type of backdoor, called Lizar. The latest version has been in use since February, and it offers a powerful set of data retrieval and lateral movement capabilities, according to an analysis published on Thursday.

“Lizar is a diverse and complex toolkit,” according to the firm. “It is currently still under active development and testing, yet it is already being widely used to control infected computers, mostly throughout the United States.”

Victims so far have included attacks on a gambling establishment, several educational institutions and pharmaceutical companies in the U.S., along with an IT company headquartered in Germany and a financial institution in Panama.

Inside FIN7’s Lizar Toolkit

The Lizar toolkit is structurally similar to Carbanak, researchers said. It consists of a loader and various plugins that are used for different tasks. Together they run on an infected system and can be combined into the Lizar bot client, which in turn communicates with a remote server.

“The bot’s modular architecture makes the tool scalable and allows for independent development of all components,” according to the analysis. “We’ve detected three kinds of bots: DLLs, EXEs and PowerShell scripts, which execute a DLL in the address space of the PowerShell process.”

The plugins are sent from the server to the loader and are executed when a certain action is performed in the Lizar client application, according to BI.ZONE.

The six stages of the plugins’ lifecycle are as follows:

- The user selects a command in the Lizar client application interface;
- The Lizar server receives the information about the selected command;
- The server finds a suitable plugin from the plugins directory, then sends it to the loader;
- The loader executes the plugin and stores the result of the plugin’s execution in a specially allocated area of memory on the heap;
- The server retrieves the results of plugin execution and sends them on to the client; and
- The client application displays the plugin results.

The plugins are variously designed to load other tools like Mimikatz or Carbanak, retrieve information from the victim machine, take screenshots, harvest credentials, retrieve browser histories, and more.

The specific bot commands are as follows:

- Command Line – get CMD on the infected system;
- Executer – launch an additional module;
- Grabber – run one of the plugins that collect passwords in browsers, Remote Desktop Protocol and Windows OS;
- Info – retrieve information about the system;
- Jump to – migrate the loader to another process;
- Kill – stop plugin;
- List Processes – get a list of processes;
- Mimikatz – run Mimikatz;
- Network analysis – run one of the plugins to retrieve Active Directory and network information;
- New session – create another loader session (run a copy of the loader on the infected system);
- Rat – run Carbanak; and
- Screenshot – take a screenshot.

The Lizar server application, meanwhile, is written using the .NET framework and runs on a remote Linux host, researchers said. It supports encrypted communications with the bot client.

“Before being sent to the server, the data is encrypted on a session key with a length ranging from 5 to 15 bytes and then on the key specified in the configuration (31 bytes),” researchers explained. “If the key specified in the configuration (31 bytes) does not match the key on the server, no data is sent from the server.”

Cybercriminals Posing as Security Researchers

The impressively ironic tactic of posing as a security outfit while contributing to, well, insecurity is not a new idea, even for FIN7. In the past, BI.ZONE has observed it pushing Carbanak under the guise of the package being a tool from cybersecurity stalwarts Check Point Software or Forcepoint.

Earlier this year, a North Korean advanced persistent threat group (APT) called Zinc, which has links to the more notorious APT Lazarus, mounted two separate attacks targeting security researchers.

In January, the group used elaborate social-engineering efforts through Twitter and LinkedIn, as well as other media platforms like Discord and Telegram, to set up trusted relationships with researchers by appearing to themselves be legitimate researchers interested in offensive security.

Specifically, attackers initiated contact by asking researchers if they wanted to collaborate on vulnerability research together. They demonstrated their own credibility by posting videos of exploits they've worked on, including faking the success of a working exploit for an existing, patched Windows Defender vulnerability that had been exploited as part of the massive SolarWinds attack.

Eventually, after much correspondence, attackers provided the targeted researchers with a Visual Studio Project infected with malicious code that could install a backdoor onto their system. Victims also could be infected by following a malicious Twitter link.

Security researchers infected in those attacks were running fully patched and up-to-date Windows 10 and Chrome browser versions, according to Google TAG at the time, which signaled that hackers likely were using zero-day vulnerabilities in their campaign.

Zinc was back at it in April, using some of the same social-media tactics but adding Twitter and LinkedIn profiles for a fake company called "SecuriElite," which purported to be an offensive security firm located in Turkey. The company claimed to offer pen tests, software-security assessments and exploits, and purported to actively recruit cybersecurity personnel via LinkedIn.

Source: https://threatpost.com/fin7-backdoor-ethical-hacking-tool/166194/