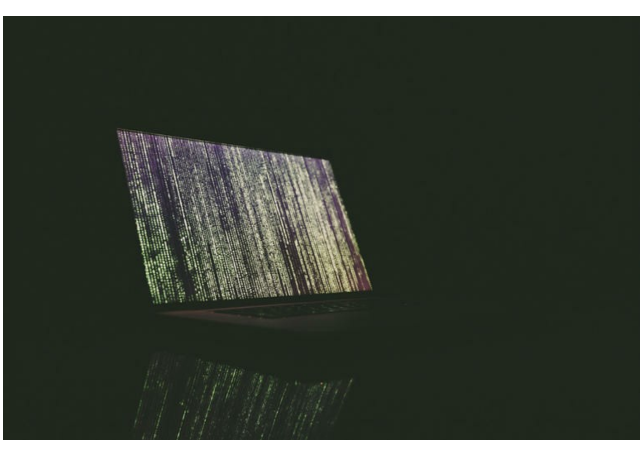
MUST READ: This new variant of Mirai botnet malware is targeting network-attached storage devices

Carbanak hackers pivot plan of attack to target banks, the enterprise

The cyberattackers are using a fresh set of techniques to infiltrate the enterprise.

By Charlie Osborne for Zero Day | October 10, 2017 -- 08:50 GMT (09:50 BST) | Topic: Security



Markus Spiske / CC

Cyberattackers behind the theft of billions worldwide have changed their plan of attack in targeting businesses across the globe.

FIN7, linked to the Carbanak Trojan, is a financially-motivated threat group which has been linked to a string of attacks against companies and financial institutions in the past.

In 2015, Kaspersky researchers uncovered the groups' involvement in the theft of over $1 billion from banks over the span of two years in roughly 30 countries.

The Carbanak Trojan was at the heart of the attacks. The banks were infected through spear phishing emails and the group took advantage of poorly patched, network-misconfigured systems.

Once a system was infected, the malware provided the conduit for FIN7 to covertly spy on staff, watch how they transferred cash, and then mimic the techniques to transfer funds fraudulently without detection.

FIN7 has been connected to attacks using legitimate software which are aimed at business credentials, and recently, the hacking group has been linked to campaigns against US restaurant chains.

Cybersecurity researchers from Seattle-based Icebrg have now uncovered a change in attitude from FIN7, which has ramped up its infiltration techniques to avoid detection.

In a blog post earlier this week, researchers Alex Sirr and Spencer Walden said that FIN7 has recently focused on improving their phishing documents, with the latest update receiving a concerning initial detections on VirusTotal of 0/59 and 1/59 for RTF and DOCX formats respectively -- which means that traditional antivirus software may not be enough to pick up malicious code embedded in a seemingly legitimate business email.

"While the newly observed malicious documents do not represent a "new" attack methodology, the change of payload may cause detection issues for legacy signatures and heuristic detections which utilize overly strict detection mechanisms, lacking in durability or layered coverage," the researchers said.

The threat actors use phishing to gain an initial foothold into a corporate network. Once complete, the group then paves their way through to Point of Sale (PoS) systems in order to steal credit card data, which can then be used in identity theft or potentially card cloning, should the information not be encrypted well.

FIN7 now uses a modified payload with an embedded file type for the first wave of attack. In the past, the cyberattackers have been spotted using malicious shortcut files (LNK) or visual basic scripts (VBS or VBE) to lay the trap for remote code execution.

These files were embedded into malicious documents using the Windows Object Linking and Embedding (OLE) framework.

However, it appears the hackers are now switching from LNK files to OLE embedded CMD files. These files are underlain with JScript, and writes a "tt.txt" files to the victim's home directory. The script then uses the JScript engine on the file, also leading to code execution, but is more difficult to spot.

In addition, FIN7's custom backdoor, HALFBAKED, has evolved. In the newest version, changes have been made to obfuscation techniques.

Originally, HALFBAKED utilized base64 encoding, stored in a string array variable called "srcTxt." Now, this name is obfuscated and the string is broken up into multiple strings.

The backdoor is also equipped with a command called "getNK2" which is designed to covertly pull a victim's full Microsoft Outlook email client auto-complete list, which suggests the threat group is keen to acquire as many new targets as possible.

"Detection authors must make trade-offs to optimize signature performance; narrow signatures lead to high fidelity detections, but risk missing changes in actor behaviors, meanwhile broader detection patterns provide better coverage, at the risk of more false positives," the researchers note. "Combatting a well-resourced and adaptive adversary requires a layered approach of both signature styles."

Must-have mobile apps to encrypt your texts... SEE FULL GALLERY
1 - 5 of 9 NEXT

PREVIOUS AND RELATED COVERAGE

Cybercrime gang uses Google services for malware command and control

Gang behind multiple cyberattacks on banks and financial institutions has found a new way to manage its activities.

Carbanak hacking group steal $1 billion from banks worldwide

Carbanak malware offered criminals the chance to steal up to $10 million per heist.

New Trojan malware attack targets restaurant chains

Dubbed Bateleur, this malware uses with macro-laden phishing emails that allow attackers to take screenshots, steal passwords, and more.

RELATED TOPICS: SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Charlie Osborne for Zero Day | October 10, 2017 -- 08:50 GMT (09:50 BST) | Topic: Security