SentinelLABS
(https://www.sentinelone.com/labs/)

Search ...

ADVANCED PERSISTENT THREAT
(HTTPS://WWW.SENTINELONE.COM/LABS/CATEGORY/ADVANCED-PERSISTENT-THREAT/)

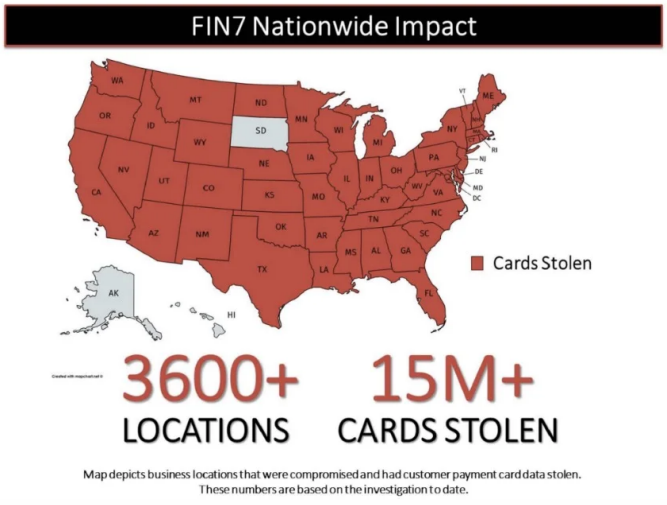
Deep Insight into “FIN7” Malware Chain: From Office Macro Malware to Lightweight JS Loader

VITALI KREMEZ (HTTPS://WWW.SENTINELONE.COM/BLOG/AUTHOR/VITALIK/) / OCTOBER 3, 2019 (HTTPS://WWW.SENTINELONE.COM/BLOG/2019/10/)

Vitali Kremez dissecting the ‘Fin7’ malware chain, which leverages malicious Office Macros and lightweight JS Loader scripts.

“FIN7” is a financially motivated advanced persistent group (https://www.sentinelone.com/blog/what-are-advanced-targeted-attacks/) operating out of Eastern Europe. Since 2015, this group has continued to be extremely successful and formidable targeting various businesses seeking large-scale point-of-sale (https://www.sentinelone.com/blog/fin6-frameworkpos-point-of-sale-malware-analysis-internals/) (PoS) compromises and network intrusion impacting global enterprises. The group is also known and notorious for its stealthy techniques and sophisticated and persistent approach.

Global corporations impacted by the group are primarily part of the restaurant, gaming, and hospitality industries. Some of the victims of this group include such restaurant chains as Chipotle Mexican Grill, Chili’s, and Arby’s.



Source: DOJ

Most interestingly, this group used a front company “Combi Security” (reportedly based in Russia and Israel) to recruit various hackers to join their activities. This front company allowed the group to sustain their hacking activities and truly professionalized their hacking approach.

Despite the previous arrests of three members of the FIN7 group in January 2018, the group and/or its remnants still remained active on the financial crime (https://www.sentinelone.com/blog/ecommerce-security-13-best-practices-to-prevent-threats/) landscape.

Exploring the VirusTotal Dataset | An Analyst’s Guide to Effective Threat Research (https://www.sentinelone.com/labs/exploring-the-virustotal-dataset-an-analysts-guide-to-effective-threat-research/)

AUGUST 29, 2024

LABScon23 Replay | Black Magic – Influence Operations in the Open and At-Scale in Hungary (https://www.sentinelone.com/labs/labscon23-replay-black-magic-influence-operations-in-the-open-and-at-scale-in-hungary/)

AUGUST 21, 2024

Xeon Sender | SMS Spam Shipping Multi-Tool Targeting SaaS Credentials (https://www.sentinelone.com/labs/xeon-sender-sms-spam-shipping-multi-tool-targeting-saas-credentials/)

AUGUST 19, 2024

LABS CATEGORIES

Crimeware (https://www.sentinelone.com/labs/category/crimew

Security Research (https://www.sentinelone.com/labs/category/security-research/)

Advanced Persistent Threat (https://www.sentinelone.com/labs/category/advanced-persistent-threat/)

Adversary (https://www.sentinelone.com/labs/category/adversa

LABScon (https://www.sentinelone.com/labs/category/labscon

Security & Intelligence (https://www.sentinelone.com/labs/category/security-intelligence/)

Source: DOJ

It is notable that the group still deploys lightweight JavaScript backdoor with communication over HTTPS mimicking Content Delivery Network (CDN) domains.

Additionally, they still leverage JavaScript backdoor via renamed `wscript.exe` with the actual JavaScript code called “errors.txt,” for example.

FIN7: From First-Stage Microsoft Office VBA Macro Loader to JS Loader

The FIN7 Microsoft document loaders do not rely on any exploits but simply require a social engineering trick (https://www.sentinelone.com/blog/phishing-revealing-vulnerable-targets/) to “Enable Content” to activate macros. Notably, to avoid process whitelisting (https://www.sentinelone.com/blog/can-whitelisting-win-advanced-persistent-threats/) of `wscript`, the macro logic copies the original JavaScript execution engine `wscript.exe` in `%LOCALAPPDATA%` and leverages a possible anti-analysis routine of checking the system drive size via `GetDrive.TotalSize` of more than 2456 bytes to possibly thwart anti-sandbox check.

The actual obfuscated Javascript backdoor is stored in UserForm object, which is also written to a disc as “errors.txt” in `%TEMP%`. The final execution of the backdoor is performed via this following command:

```
%LOCALAPPDATA%mses.exe //b /e:jscript %temp%errors.txt
```

Once it is done, the document macro (https://www.sentinelone.com/news/how-can-obfuscated-macro-malware-be-located-and-removed/) runs a message box displaying “Decryption error” via `MsgBox("Decryption error")`.

Reversing Steps:

1. Extract the VBA macro via olevba (https://github.com/decalage2/oletools/wiki/olevba);

2. Debug in Office VBA to retrieve decoded script;

3. Extract and prettify obfuscated JavaScript backdoor from userform object;

4. Modify JS code close to `eval()` and run script via Internet Explorer debugger, for example;

5. Debug, extract and beautify the full FIN7 JS backdoor.

FIN7 JS Loader/Backdoor XOR Encryption & Custom Encoding

The `crypt_controller` function accepts two parameters of *type* and *request*.

a. If *type* parameter equals “decrypt”, the *request* is processed via `decodeURIComponent` splitting the request with separator `")*("` and then retrieving `encryption_key(second element[1])` from split request. If there’s no encryption_key split, it pulls it as a random value via `(Math.floor(Math.random() * 9000) + 1000).toString().split("");`.

The decoding routine is a simple XOR loop decoding the content as follows joining the `result_string` via `.join` command.

```
var output = [];


    for (var i = 0; i < request.length; i++) {

        var charCode = request.charCodeAt(i) ^

encryption_key[i % encryption_key.length].charCodeAt(0);

        output.push(String.fromCharCode(charCode));
    }
```

b. If *type* parameter equals “encrypt”, the `result_string` is joined with `")*("` and passed to `encodeURIComponent`.

FIN7 Second-Stage Machine & Network Profiling Script

In the aftermath of the initial call, the group deploys a custom “profiling” script meant to fingerprint the machine and the network environment more closely.

The malware checks for the presence of virtual machine, queries active directory, operating system, screen resolution, user account control (UAC) level, and retrieves a process list.

Finally, it formats the data and appends to “action=add_info” request, which is sent to the server.

Indicators of Compromise (IOCs):

Microsoft Office First-Stage VBA Macro “.doc”

Documents:

SHA256:

6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bff fd5017ca82

SHA256:

f5f8ab9863dc12d04731b1932fc3609742de68252c706952f31894 fc21746bb8

SHA256:

63ff5d9c9b33512f0d9f8d153c02065c637b7da48d2c0b6f7114de ae6f6d88aa

C2:

googleapi-cdn[.]com

bing-cdn[.]com

cisco-cdn[.]com

Recent Microsoft Office First-Stage VBA Macro “.xlsb”

Documents:

SHA256:

5fa5970548b43ae7d93d758a1eef1f12fd76891e36538e3ac170d5 ab30906b5c

SHA256:

60dfe419dcba6dfe16d24f663b3393deeffdedbe4da468be63c63e c4b914d485

SHA256:

2ce1cfc137c0bcc82577cc77074c82154d81a7370491c85d43622a f5186ef058

Recent C2:

realtek-cdn[.]com

FIN7 (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/FIN7/)

REVERSE ENGINEEERING (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/REVERSE-ENGINEEERING/)

VITALI KREMEZ (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/VITALI-KREMEZ/)

ZERO2HERO (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/ZERO2HERO/)

SHARE

(https://www.facebook.com/sharer.php?u=https://www.sentinelone.com/labs/deep-insight-into-fin7-malware-chain-from-office-macro-malware-to-lightweight-js-loader/) (https://www.linkedin.com/shareArticle?mini=true&url=https://www.sentinelone.com/labs/deep-insight-into-fin7-malware-chain-from-office-macro-malware-to-lightweight-js-loader/) (https://www.sentinelone.com/wp-content/uploads/pdf-generator-pro-cache/2024/05/deep-insight-into-fin7-malware-chain-from-office-macro-malware-to-lightweight-js-loader.pdf) (mailto:?subject=Deep%20Insight%20into%20%E2%80%9CFIN7%E2%80%9D%20Malware%20Chain%3A%20From%20Office%20Macro%20Malware%20to%20Lightweight%20JS%20Loader&body=https%3A%2F%2Fwww.sentinelone.com%2Flabs%2Fdeep-insight-into-fin7-malware-chain-from-office-macro-malware-to-lightweight-js-loader%2F)

VITALI KREMEZ (https://www.sentinelone.com/blog/author/vitalik/)

Vitali Kremez is a strategic advisor for SentinelLabs. He specializes in researching and investigating complex cyberattacks, network intrusions, data breaches, and hacking incidents mainly emanating from the Eastern European cybercriminal ecosystem. He has earned the majority of major certifications available in information technology, information security, and digital forensics fields.

(https://www.vkremez.com/) (https://www.linkedin.com/in/vitali-kremez-021905104/) (https://twitter.com/vk_intel)

PREV

Info Stealers | How Malware Hacks Private User Data (https://www.sentinelone.com/labs/info-stealers-how-malware-hacks-private-user-data/)

NEXT

Writing Malware Configuration Extractors for ISFB/Ursnif (https://www.sentinelone.com/labs/writing-malware-configuration-extractors-for-isfb-ursnif/)

RELATED POSTS

ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware (https://www.sentinelone.com/labs/attacking-critical-infrastructure-with-ransomware/)

JUNE 26 2024

Unmasking I-Soon | The Leak That Revealed China’s Cyber Operations (https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/)

FEBRUARY 21 2024

ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals (https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/)

JANUARY 22 2024