Blue Team Level 1 Certification (Standard)

Introduction to BTL1
- ~~Welcome to Blue Team Level 1!~~ 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN
- ~~Introduction to Security Fundamentals~~ 1 Topic
- ~~Soft Skills~~ 7 Topics
- ~~Security Controls~~ 5 Topics | 1 Quiz
- ~~Networking 101~~ 6 Topics | 1 Quiz
- ~~Management Principles~~ 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN
- ~~PA1) Introduction to Emails and Phishing~~ 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~ 10 Topics | 2 Quizzes
- ~~PA3) Tactics and Techniques Used~~ 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~ 8 Topics | 2 Quizzes
- ~~PA5) Analysing URLs, Attachments, and Artifacts~~ 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions 12 Topics | 1 Quiz
- PA7) Report Writing 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN
- TI1) Introduction to Threat Intelligence 7 Topics
- TI2) Threat Actors & APTs 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns 6 Topics | 1 Quiz
  - Section Introduction, Global Campaigns
  - Types of Malware Used by Threat Actors
  - Global Campaign: Trickbot
  - Global Campaign: Sodinokibi
  - Global Campaign: Magecart

Global Campaign: Sodinokibi

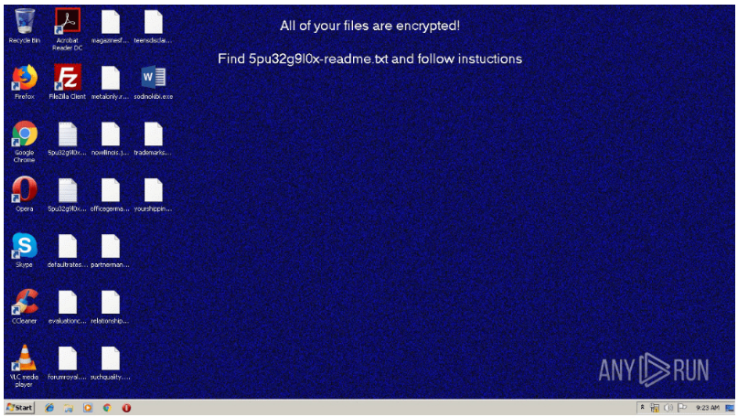
Sodinokibi (also known as Sodin or REvil) is one of the malwares that is gaining strength at this moment, since, despite having appeared in mid 2019, it has become one of the most commonly used ransomware in the last year. Thought to be developed by the APT "Gold Garden" (creators of the discontinued ransomware GandCrab) and "Gold Southfield", it is a virus specialized in data encryption that, through vulnerabilities in applications such as Oracle WebLogic Server (CVE-2019-2725) or the same Windows operating system (CVE-2018-8453) is capable of encoding absolutely all files within the hard drive of a computer, preventing the victim from accessing these and allowing the attacker to request a fairly high payment for the recovery of this information in no more than 4 days (payments varying between $2500 and $5000 per infection)

HOW DOES IT WORK?

Sodinokibi attacks work through a .ZIP file that is obtained directly from the internet (Attackers often use spam campaigns or infect websites to get targets to download this file). Once the .ZIP file is downloaded to the computer and executed (the moment the infected user tries to open it), the macros within the file are set up, starting the process of encrypting the files. In this process, ransomware specifically looks for files that are "important" to the user and do not compromise the proper operation of the system, which means files with the following extensions:

.jpg, .jpeg, .raw, .tif, .png, .bmp, .3dm, .max, .accdb, .db, .mdb, .dwg, .dxf, .cpp, .cs, .h, .php, .asp, .rb, .java, .aaf, .aep, .aepx, .plb, .prel, .aet, .ppj, .gif, and .psd.

Once the files are encrypted, the computer's wallpaper is changed alerting the victim to look for a text file that has the instructions for rescuing the information, and a website that allows a test "decryption".

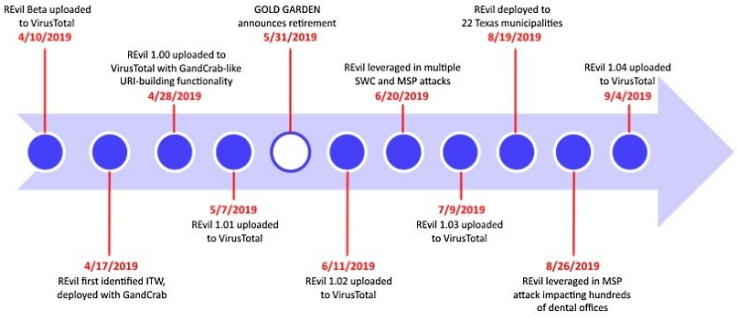


Source: Any Run

Global Campaign: Emotet
Activity) End of Section Review, Global Campaigns
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

Source: Any Run

EVOLUTION AND UPDATES



Source: SecureWorks

- **The Beginning:**

Sodinokibi formally appears on the map on April 17th, 2019, where through a ZIP file embedded with malicious JavaScript it tried to infect some machines all over the internet (this initial attack was based on malspam campaigns). Later, between April 26th and May 3rd, through a vulnerability in Oracle WebLogic Server (CVE-2019-2725) it was used against a large number of computers. In this attack, user interaction was no longer necessary. Instead, through the server failure, the attackers were able to install ransomware directly on the target machines. In fact, this malware was used in several test campaigns deployed from April 10th to May 7th. During this initial period, Sodinokibi was accompanied by the discontinued ransomware GandCrab (versions 5.2 and 6.0), apparently with the purpose of infecting those computers in which Sodinokibi failed, and thus be able to demand payments to the victims.

- **July 3rd, 2019:**

Sodinokibi receives an update that allows it to take advantage of the Windows vulnerability (CVE-2018-8453), which, through the Win32k.sys program allows privilege escalation, a tactic that Sodinokibi utilized to increase its encryption power, now making use of two methods: **AES-256-CTR** for encrypting the private keys of the private-public key pair (generated locally on the user's machine), and **Salsa20** for encrypting the user's files.

Thanks to this update two keys are now necessary to decrypt the information captured by Sodinokibi.

- **September 3rd, 2019:**

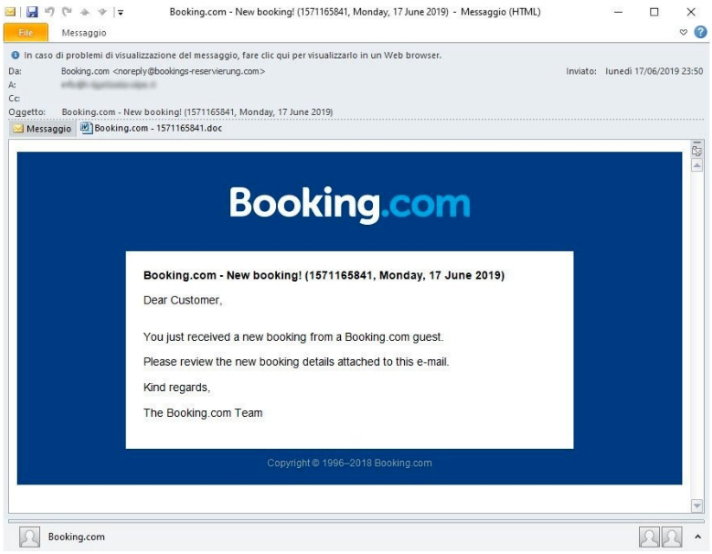
Sodinokibi infects WordPress servers. By using the JavaScript injection method, the attackers were able to insert malicious code into the website so they could infect more people. In these cases, the attackers used the Q&A or the Downloads section, placing malicious links that included the ransomware installation file. (Italian WINRAR was one of the affected websites)

- **January 23rd, 2020:**

Attackers become more aggressive by not receiving ransomware payments, filtering out information obtained from victims who have been unwilling to contact them to pay the ransom payment.

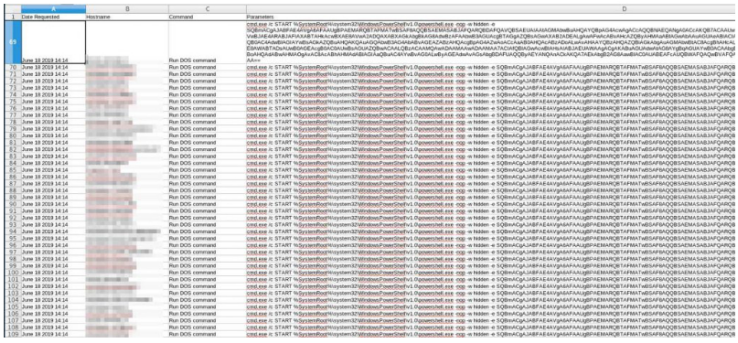
INFECTION PROCESS

The ransomware spreading process has many delivery methods, varying from malspam campaigns with malicious attachments to exploiting flaws in remote desktop services. Originally the spreading behavior of this malware was the same as many other common virus. Through spam campaigns, they would send a ZIP file or a document (.doc, .pdf, etc.) infected with JavaScript code which allowed the installation of Sodinokibi in the background thanks to the PowerShell. The emails and files would look like this:



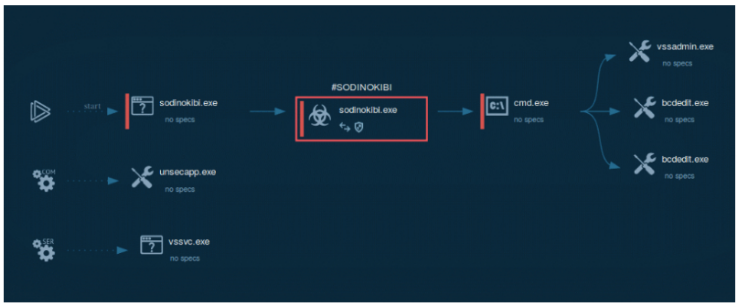
Source: Bleepingcomputer

Malicious spam campaigns to deliver Microsoft Office files with malicious macros is a pretty standard delivery method, but Sodinokibi didn't stop there. Through new vulnerabilities and zero-day exploits, the malicious actors wanted to improve their malware and thus have more control over their victims, by reducing the need for human interaction to infect a system. At this point, Sodinokibi starts to infect remote desktop services and use vulnerabilities like the previously mentioned CVE-2019-2725. The below image from BleepingComputer shows a network of infected computers that were compromised via Remote Desktop, and PowerShell is used to download Sodinokibi from a malicious domain.



Source: Bleepingcomputer

Once a system is infected, the malware removes all Windows Shadow Copies from the system files (via **vssadmin.exe**) and disables Windows recovery via **bcdedit.exe.** All of this is done with the purpose of making it more difficult for the victim to recover the files once the encryption has been performed.



Source: Any Run

Immediately after the process of deleting the files from the system, Sodinokibi generates a whole procedure to request the rescue of the information.

It starts by creating an identifier for each infected computer, this in order to use it to create a unique payment URL for each victim **(this address is made by using the serial number of the hard disk and the CPUID, these two parameters serve as seeds to generate a CRC32 hash, which will be the URL)**, then proceeds with the creation of public/private keys for the file encryption process, continuing with the generation of a random extension for these

public/private keys for the file and python process, continuing with the generation of a random attacker for these encrypted files, and ending with the creation of a rescue document and changing the wallpaper to make the attack visible.

As previously mentioned, Sodinokibi generates two pairs of public/private session keys, these will be used for the encryption and later decoding of the information; where one pair will be used in the encryption of the private key generated in the communication process with the computer **(sk_key** and **0_key)** and the other will be used in the private key used for the encryption of the files **(pk_key)**. (Both public keys are generated by the attacker).

Once the encryption keys have been created, ransomware proceeds to use the **rnd_ext** file to place an extension on the encrypted files **(This address is a randomly generated string of lowercase letters (a-z) and numbers (0-9) of about five or ten characters in length)**.

After obtaining all this data, Sodinokibi proceeds to encrypt the computer files. Its process starts by checking one by one all the directories on the hard disk, looking for not listed folders in the ransomware white list, if it finds any it will ignore it and continue looking for those not listed (these exceptions are usually directories that have files needed for the correct system operation).

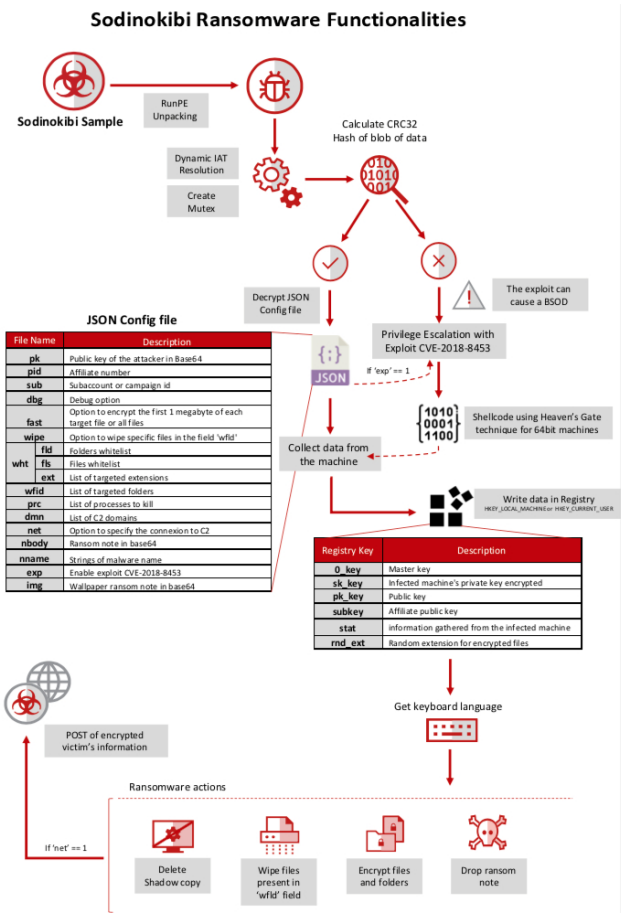
```
"wht": {
    "ext": [ "msstyles", "icl", "idx", "rtp", "sys", "nomedia", "dll", "hta", "cur", "lock", "cpl", "ics",
             "hlp", "com", "spl", "msi", "key", "mpa", "rom", "drv", "bat", "386", "adv", "diagcab", "mod",
             "scr", "theme", "ocx", "prf", "cab", "diagcfg", "msu", "cmd", "ico", "msc", "ani", "icns",
             "diagpkg", "deskthemepack", "wpx", "msp", "bin", "themepack", "shs", "nls", "exe", "lnk", "ps1",
             "ldf"
    ],
    "fld": [ "msocache", "$windows.~ws", "system volume information", "intel", "appdata", "perflogs",
             "programdata", "program files (x86)", "$windows.~bt", "windows", "mozilla", "$recycle.bin",
             "boot", "program files", "windows.old", "google", "application data", "tor browser"
    ],
    "fls": [ "desktop.ini", "ntuser.dat", "thumbs.db", "iconcache.db", "ntuser.ini", "ntldr",
             "bootfont.bin", "ntuser.dat.log", "bootsect.bak", "boot.ini", "autorun.inf"
    ]
```

Source: SecureWorks

When it finds a folder that is not on the above list, the malware proceeds to perform the following encryption process using the salsa20 stream cipher and one of the previously generated keys **(pk_key)**:

1. **Reads the file contents into a buffer**
2. **Encrypts the contents of the buffer**
3. **Writes the encrypted contents of the buffer to the original file, overwriting the original file content**
4. **Renames the original file with the previously generated random extension**

And finally, after encrypting all possible files, Sodinokibi creates the rescue note by modifying all the values obtained from the computer and changes the wallpaper of the machine to notify the victim of its situation, finishing the infection process of the Ransomware. Which, after this whole set of steps would look like this:



Source: McAfee

CONCLUSION

Sodinokibi is an effective ransomware and is ever-changing, ensuring that the operators behind Sodinokibi can continue to infect systems and make financial gains. The techniques used by this ransomware are very robust, but good security education and especially security updates can prevent many of these infections.

Previous Topic

Mark Complete

Next Topic

Back to Lesson

Privacy & Cookies Policy

Privacy - Terms