



# Teaching an Old Dog New Tricks: 2017 Magniber Ransomware Uses PrintNightmare Vulnerability to Infect Victims in South Korea

August 11, 2021

Liviu Arsene  
Endpoint & Cloud Security



- 2017 Magniber ransomware makes a comeback using the same methods: exploiting unpatched vulnerabilities on South Korean victims
- In July 2021, CrowdStrike identified Magniber ransomware attempting to use a known PrintNightmare vulnerability to compromise victims
- CrowdStrike detects and protects against both the exploitation of the PrintNightmare vulnerability and the Magniber ransomware

CrowdStrike recently observed new activity related to a 2017 ransomware family, known as Magniber, using the [PrintNightmare vulnerability](#) on victims in South Korea. On July 13, CrowdStrike successfully detected and prevented attempts at exploiting the PrintNightmare vulnerability, protecting customers before any encryption takes place.

When the PrintNightmare ([CVE-2021-34527](#)) vulnerability was disclosed, CrowdStrike intelligence assessed the vulnerability will likely be used by threat actors as it allowed for possible remote code execution (RCE) and local privilege escalation (LPE). This assessment proved accurate in light of the recent incident.

Using mitigations that target the tactics and techniques used by adversaries to compromise endpoints, the CrowdStrike Falcon® platform provides layered coverage against threats by using machine learning (on-sensor and in the cloud) and indicators of attack (IOAs) to identify malicious processes or files associated with known or unknown threats.

## A Timeline for the PrintNightmare Vulnerability

**June 8, 2021:** The PrintNightmare ([CVE-2021-1675](#)) vulnerability was initially discovered and reported to Microsoft on June 8, by security researchers working for three different companies. Their research involved attempting to bypass a previous patch addressing the “PrintDemon” ([CVE-2020-1048](#)) vulnerability.

**June 21, 2021:** While Microsoft released a patch for [CVE-2021-1675](#), as part of [Microsoft’s June 2021 Patch Tuesday](#), no additional information regarding how to exploit the vulnerability was made public. At the time, it was believed the vulnerability could only be exploited by a locally authenticated user. However, the vulnerability was elevated to Critical on June 21 by Microsoft, as it was determined it could allow for RCE.

**June 29, 2021:** Independently, one of three additional security researchers investigating a similar bug in the Windows Print Spooler service inadvertently published a proof of concept (POC) exploiting the ([CVE-2021-1675](#)) vulnerability on a GitHub repository, on June 29. While the error was shortly corrected, the GitHub repo was reportedly forked and the POC made it into the wild, potentially leading to abuse by attackers.

**July 1, 2021:** Although Microsoft addressed the [CVE-2021-1675](#) vulnerability by issuing a patch, the leaked POC exploited a different attack vector that triggered the Print Spooler vulnerability. As of July 1, several different proof of concepts exploiting the Printer Spooler vulnerability were made public. Consequently, a second CVE ([CVE-2021-34527](#)) was created on July 1, with Microsoft stating that “[CVE-2021-1675](#) is similar but distinct from [CVE-2021-34527](#).”

**July 6, 2021:** On July 6, Microsoft issued an [out-of-band \(OOB\) update](#) attempting to mitigate the [CVE-2021-34527](#) vulnerability, but hours later security researchers found that it was again possible to bypass imposed mitigations under certain conditions. Popular exploit tools, such as Metasploit and Mimikatz, [started incorporating the exploit code](#), paving the way for adversary weaponization of a yet unpatched vulnerability.

## A Primer on Magniber Ransomware

Magniber ransomware was first spotted in late 2017 targeting victims in South Korea through malvertising campaigns using the Magnitude Exploit Kit (EK). Previous Magniber campaigns went through significant efforts to only infect victims in South Korea, although in mid-2018 it was also spotted targeting victims in other Asia Pacific countries.

Magnitude Exploit Kit (EK) operators initially used the Cerber ransomware exclusively before turning to Magniber, which is believed to be the successor of Cerber. The most popular infection vector for Magniber involved the use of unpatched vulnerabilities, such as Internet Explorer exploits ([CVE-2018-8174](#), [CVE-2021-26411](#), [CVE-2020-0968](#), [CVE-2019-1367](#)) or Flash ([CVE-2018-8174](#)) vulnerabilities, infecting victims through compromised websites or drive-by downloads.

While the Magniber ransomware only seems to target the Republic of Korea, it has been active since 2017. Our Falcon OverWatch™ team also spotted more recent activity from Magniber in early February 2021, exploiting an Internet Explorer vulnerability (CVE-2020-0968) to exclusively compromise South Korean victims.

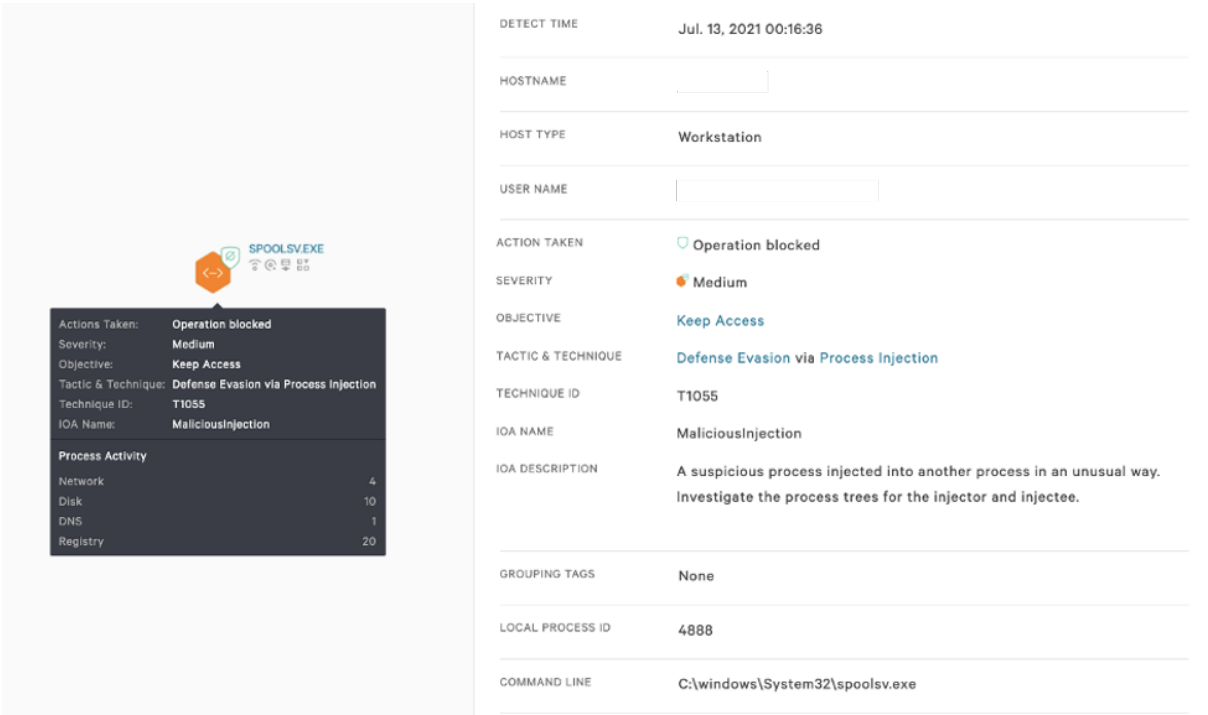
Magniber was under active development to include new obfuscation features, evasion tactics and encryption mechanisms that made the encryption more robust, showing up in sporadic campaigns over the years. Its developers also went through a significant effort to limit infections to Asia Pacific countries by including various language checks.

## PrintNightmare Meets Magniber Ransomware

The new incident involving Magniber ransomware using the recent PrintNightmare Printer Spooler vulnerability is surprising, but not uncommon considering the impact of the vulnerability. Several POCs have been in circulation since the issue was reported, and it was only a matter of time until adversaries attempted to leverage it to compromise victims and deliver malicious payloads.

The Falcon OverWatch team constantly hunts for adversary attempts trying to exploit the PrintNightmare vulnerability and recently spotted an endeavor to exploit it. A malicious dll was written to the folder `\\Device\\HarddiskVolume2\\Windows\\System32\\spool\\DRIVERS\\x64\\3\\New\\` after which it was loaded into the spoolsv.exe process. The DLL itself is associated with the Magniber ransomware and is responsible for deobfuscating the core ransomware DLL and injecting it into a remote process.

Our IOA coverage that we released as part of the PrintNightmare research successfully triggers due to this action, and prevents this operation, as seen in the screenshot below.



The screenshot displays a security dashboard with two main panels. The left panel shows a process activity summary for 'SPOOLSVEXE' with a shield icon and a red 'X' indicating a blocked operation. The right panel provides detailed IOA information.

Field	Value
DETECT TIME	Jul. 13, 2021 00:16:36
HOSTNAME	
HOST TYPE	Workstation
USER NAME	
ACTION TAKEN	Operation blocked
SEVERITY	Medium
OBJECTIVE	Keep Access
TACTIC & TECHNIQUE	Defense Evasion via Process Injection
TECHNIQUE ID	T1055
IOA NAME	MaliciousInjection
IOA DESCRIPTION	A suspicious process injected into another process in an unusual way. Investigate the process trees for the injector and injectee.
GROUPING TAGS	None
LOCAL PROCESS ID	4888
COMMAND LINE	C:\windows\System32\spoolsv.exe

**Process Activity Summary:**

- Actions Taken: Operation blocked
- Severity: Medium
- Objective: Keep Access
- Tactic & Technique: Defense Evasion via Process Injection
- Technique ID: T1055
- IOA Name: MaliciousInjection

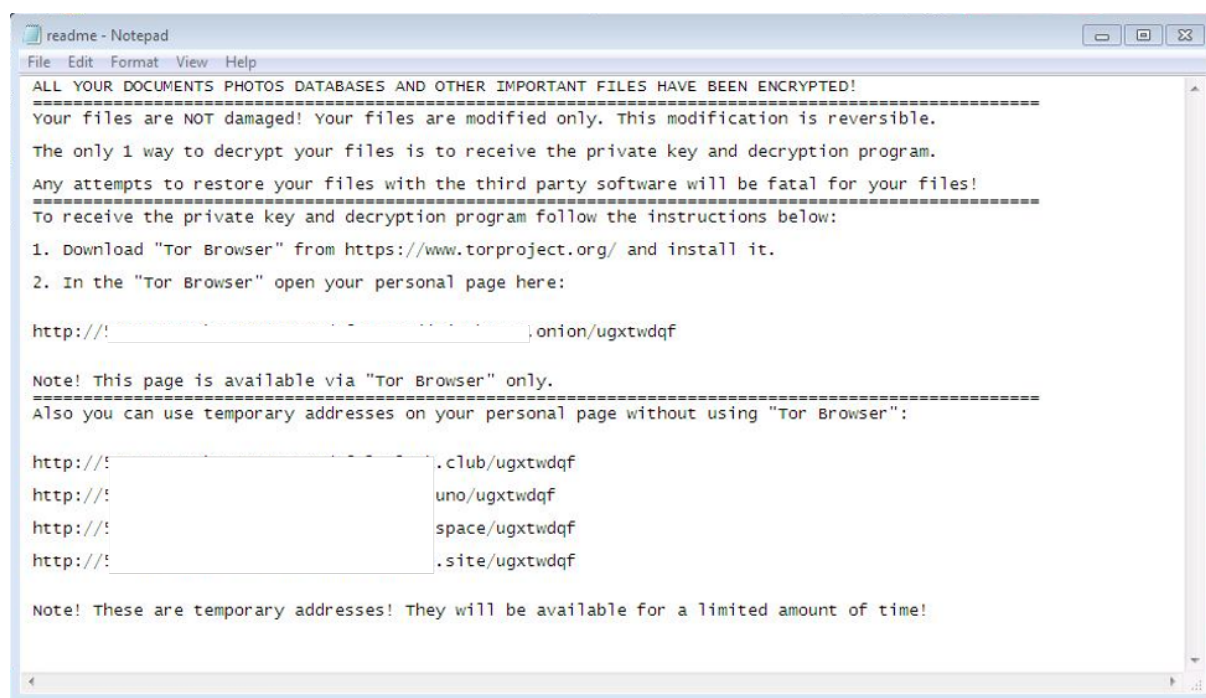
**Process Activity:**

Category	Count
Network	4
Disk	10
DNS	1
Registry	20

CrowdStrike's behavior-based detection using IOAs successfully prevented the core ransomware DLL from being injected, thwarting the malicious activity before any encryption took place on the endpoint.

Analyzing the behavior of the malicious ransomware sample reveals the same Magniber behavior observed in the past by CrowdStrike security researchers: exploiting a vulnerability, dropping an obfuscated DLL loader, injecting the loader into a process and then unpacking the cored DLL loader that performs local file traversal and encryption — which is on par with the known Magniber modus operandi.

The dropped ransom note does not reveal anything new about the operators behind this incident or the ransom payment amount. Instead, it provides instructions on contacting the ransomware operators for potential negotiation and warns victims they have a limited amount of time to contact them for decryption before the links expire.



## CrowdStrike Falcon Protection

CrowdStrike Falcon takes a layered approach to protecting endpoints that are most valuable to organizations by employing machine learning and behavior-based protection. The critical Windows Print Spooler vulnerability, PrintNightmare, is something that potentially affects all Windows hosts, which is why CrowdStrike customers are encouraged to review their prevention policies in accordance with best practices and get Falcon Spotlight™ vulnerability management to identify risks related to this. If you are not a customer, you can start a free trial of [Falcon Spotlight](#) today.

CrowdStrike Falcon leverages machine learning and IOAs to identify malicious behavior of processes or files when dealing with new or unknown threats. [This video](#) demonstrates Falcon's capabilities to successfully detect and block the Magniber ransomware DLL. First, learn how Falcon detects Magniber DLL using cloud machine learning written to disk and when injected into a remote process. Then, see a demo of Falcon's ability to block the Magniber ransomware, when all prevention and protection policies are enabled according to best practices. The Falcon sensor immediately blocks the malicious Magniber behavior, protecting the endpoint.

CrowdStrike continuously monitors the tactics, techniques and procedures (TTPs) associated with over 160 identified threat actors and numerous unnamed groups and threats, and incorporates that intelligence into the Falcon platform.

CrowdStrike estimates that the PrintNightmare vulnerability coupled with the deployment of ransomware will likely continue to be exploited by other threat actors. We encourage organizations to always apply the latest patches and security updates to mitigate known vulnerabilities and adhere to security best practices to strengthen their security posture against threats and sophisticated adversaries.

## Indicators of Compromise (IOCs)

File	SHA256
Magniber Loader DLL	10b9b1d8f6bafd9bb57ccfb1da4a658f10207d566781fa5fb3c4394d283e860e 36417f0ea6d948cbd7e003b3cefbb603d886849a8c80e0999c7969b03f2b9c28 66c4f54da6542339de036872e80306f345b8572a71e782434245455e03541465 77d3b1cf6d5a0a07090cdb078dce6e3849465c9acde7e1ba66c3893fetc73d4b 9a6584a163d8c378e6f873c5544794274cce2532e91fc079b79fd73399447b03