Glupteba back on track spreading via EternalBlue exploits

labs.k7computing.com/

By admin

June 4, 2021

Glupteba malware was first seen in the year 2014 and was active till 2020 when it faded off. But recently we at K7 Labs noticed a spike in the Glupteba malware in our K7 Enterprise Security telemetry.

On analyzing the telemetry, we came across a huge number of hits for a handful of specific systems, and on pivoting further, we realised that each of those systems were hit by tools handed down from the Equation Group and Shadow Brokers, namely EternalBlue and DoublePulsar. Along with these, many of those systems had the Ranumbot malware as well. The collective presence of all of these malware families led us on to the trail of their next of kin, Glupteba.

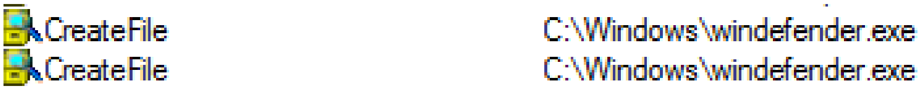
Checking the timestamp on which the malware occurrences are found in the telemetry, we noticed that they were found at regular intervals and, therefore, must have tallied with some scheduled spread from the infected system. We inferred that there must be at least one unprotected, probably unpatched, system that must have been infected and it was bombarding other protected systems on the network, a common scenario in many Enterprise networks.

The Firewall telemetry events for these systems were checked along with the corresponding IDS rules, viz. MS17-010 TRANS2 SECONDARY REQUEST and MS17-010 Echo Response. They were all found to be attempts to exploit SMB vulnerabilities. We were able to confirm that the local and remote IPs were internal, and that clearly indicates that there was attempted lateral movement within the LAN.

Basically Glupteba malware are Remote Access (Backdoor) Trojans, capable of spreading using EternalBlue exploits. The malware, once it has breached a system, looks for SMB vulnerabilities and tries to exploit them to move laterally within the LAN.

Taking a look at one of the recent Glupteba malware samples, we realise it still prefers the Go language. As a first step of its execution it copies itself to another location and creates persistence by changing the autorun values in the registry. The self-copied malware is placed in: **C:\Windows\rss\csrss.exe**

Csrss.exe drops a file named *windefender.exe* which is the Ranumbot malware, another backdoor capable of establishing remote connections and exfiltrating system information.

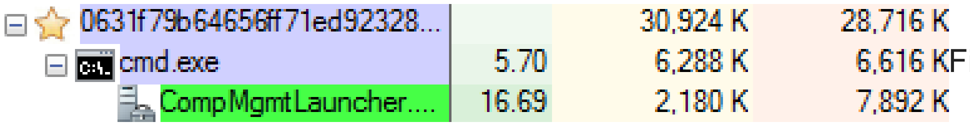


```
CreateFile                    C:\Windows\windefender.exe
CreateFile                    C:\Windows\windefender.exe
```

Figure 1: Dropped file location

This Glupteba malware attempts to evade detection on Windows Defender by modifying the registry at *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths* to add exclusions to the paths wherever it is located, and uses the command line utility to bypass the default firewall.

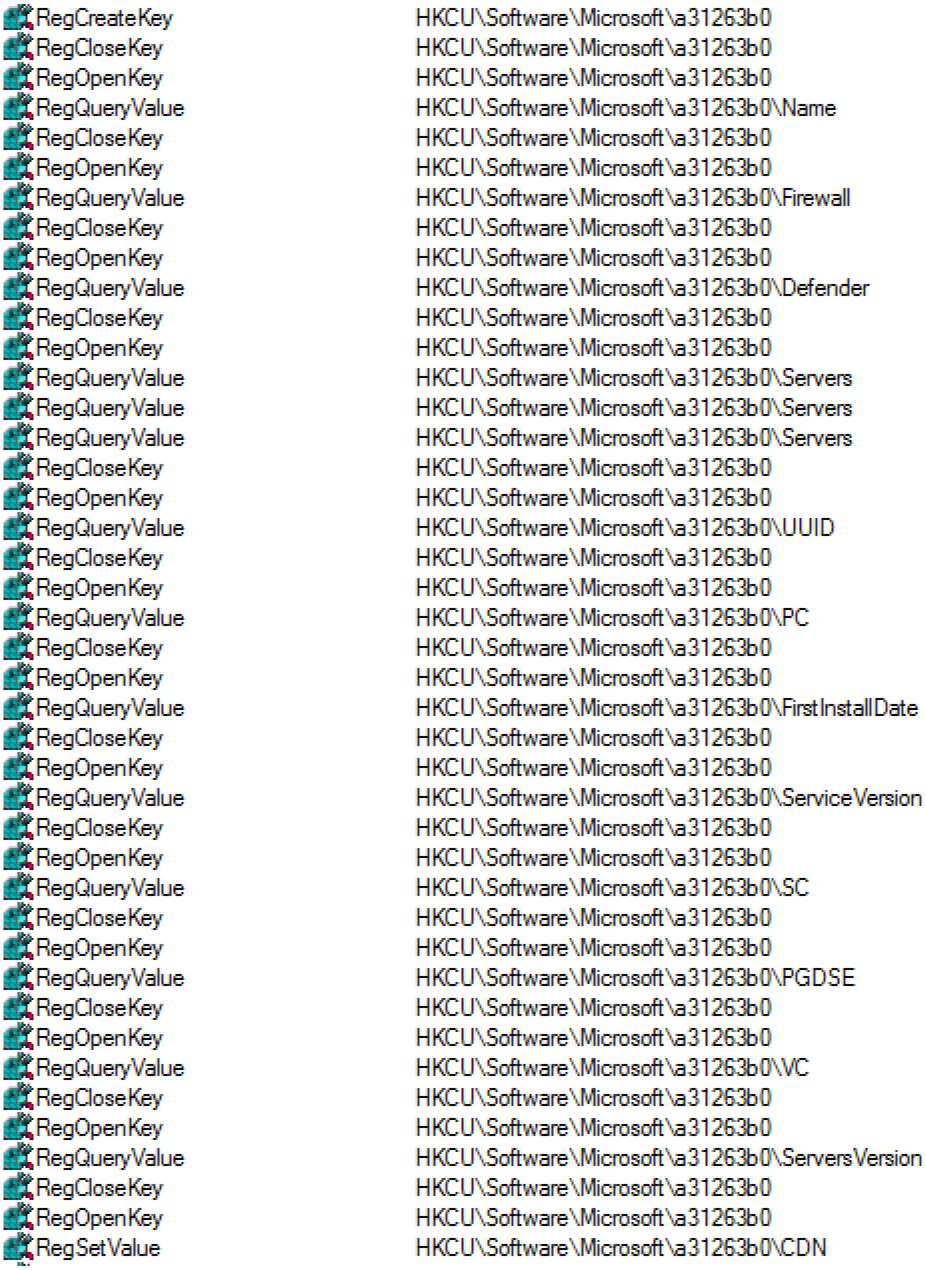
The registry *HKCU\Software\Classes\mscfile\shell\open\command* with default key value is created by the malwarein order to abuse CompMgmtLauncher.exe and bypass UAC (User Account Control). Consequently, an unchallenged execution or download of further payload is enabled.



```
⊟ 0631f79b64656ff71ed92328...            30,924 K    28,716 K
   ⊟ cmd.exe                    5.70      6,288 K     6,616 K
        CompMgmtLauncher....   16.69      2,180 K     7,892 K
```

Figure 2: Abuses CompMgmtLauncher.exe to bypass UAC

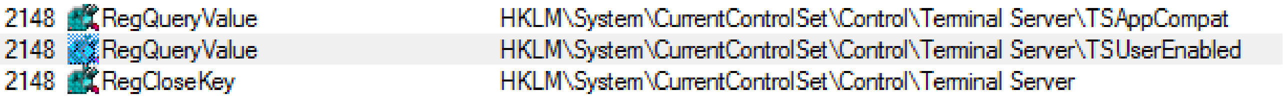
The malware collects details about the system and stores the configuration information in the registry key *HKCU\Software\ Microsoft\a31263b0*. Some of the system information that will be POSTed to the C2 include build_number, firmware_type, mac, machine_guid, secure_boot, etc, along with the list of softwares installed in the machine. The consumption of this registry key along with a previously predominant name “TestApp”, has been seen quite a lot amongst Glupteba malware, and can definitely be considered as an Indicator of Compromise (IoC). The purpose of storing the data this way is that it can be used by the malware in later stages of the infection chain.



```
RegCreateKey      HKCU\Software\Microsoft\a31263b0
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Name
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Firewall
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Defender
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Servers
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Servers
RegQueryValue     HKCU\Software\Microsoft\a31263b0\Servers
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\UUID
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\PC
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\FirstInstallDate
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\ServiceVersion
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\SC
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\PGDSE
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\VC
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegQueryValue     HKCU\Software\Microsoft\a31263b0\ServersVersion
RegCloseKey       HKCU\Software\Microsoft\a31263b0
RegOpenKey        HKCU\Software\Microsoft\a31263b0
RegSetValue       HKCU\Software\Microsoft\a31263b0\CDN
```

Figure 3: Stores configuration information in HKCU\Software\Microsoft\a31263b0

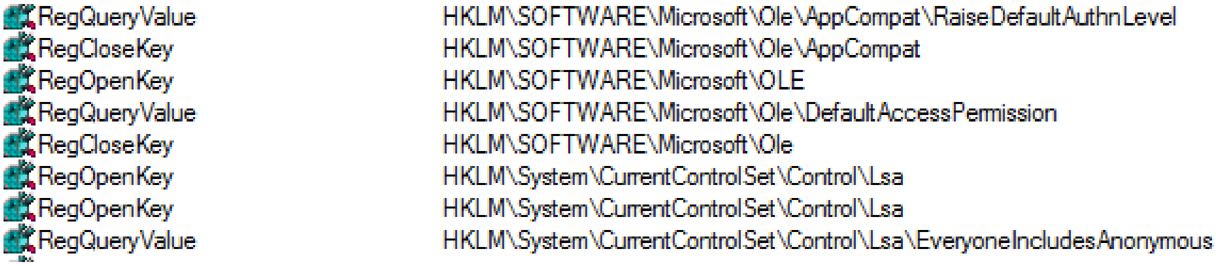
The malware uses the registry key *TSAppCompat* to check if the system is running in application compatibility mode and the registry key *TSUserEnabled,* to check if the users can log on to the terminal server



```
2148  RegQueryValue     HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat
2148  RegQueryValue     HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled
2148  RegCloseKey       HKLM\System\CurrentControlSet\Control\Terminal Server
```

Figure 4: Remote connection query

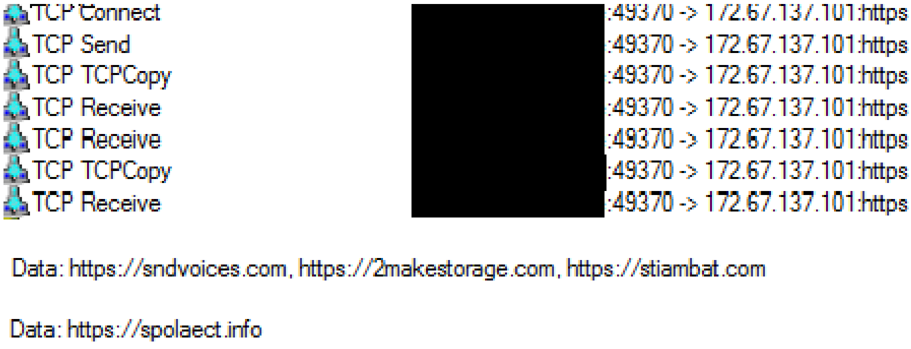
It then defines a default access permission list for the computer using the *DefaultAccessPermission* and *EveryoneIncludesAnonymous* registries to allow anyone to login without a password.



```
RegQueryValue    HKLM\SOFTWARE\Microsoft\Ole\AppCompat\RaiseDefaultAuthnLevel
RegCloseKey      HKLM\SOFTWARE\Microsoft\Ole\AppCompat
RegOpenKey       HKLM\SOFTWARE\Microsoft\OLE
RegQueryValue    HKLM\SOFTWARE\Microsoft\Ole\DefaultAccessPermission
RegCloseKey      HKLM\SOFTWARE\Microsoft\Ole
RegOpenKey       HKLM\System\CurrentControlSet\Control\Lsa
RegOpenKey       HKLM\System\CurrentControlSet\Control\Lsa
RegQueryValue    HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
```

Figure 5: Permission for anonymous user to login

A malicious network connection is made to 172.67.137.101 and to “hxxps://sndvoices.com”, “hxxps://2makestorage.com”, “hxxps://stiambat.com”, “hxxps://spolaect.info”. All of these connections attempted are malicious sites to which the exfiltrated data can be sent.



```
TCP Connect    [redacted]:49370 -> 172.67.137.101:https
TCP Send                 :49370 -> 172.67.137.101:https
TCP TCPCopy              :49370 -> 172.67.137.101:https
TCP Receive              :49370 -> 172.67.137.101:https
TCP Receive              :49370 -> 172.67.137.101:https
TCP TCPCopy              :49370 -> 172.67.137.101:https
TCP Receive              :49370 -> 172.67.137.101:https

Data: https://sndvoices.com, https://2makestorage.com, https://stiambat.com

Data: https://spolaect.info
```

Figure 6: Malicious connection

Trying to connect to *hxxps://blinkroast.info/c544b71e73e7595b36b20b7fcb8b4204/watchdog.exe* failed. The URL not being active anymore, we were not able to grab the file for further analysis.

Glupteba’s infection vectors in the past have included downloading pirated software, fake installers or adware. Once the malware has entered the system it looks for a specific list of vulnerabilities and uses them for lateral movement to enter into other systems connected in the network. In our case it is very evident that this Glupteba malware attempts to exploit SMB vulnerabilities to move laterally within the LAN.

Here at K7, proactively monitoring our K7 Ecosystem Threat Intelligence, we were able to see that Glupteba is back on active mode. Installing a reputed product like **K7 Endpoint Security** will keep you protected from all kinds of threats.

Indicators Of Compromise(IOCs)

MD5	K7 Detection Name
1a7e7794c44762d411d383fac32d45f2	Trojan (0057c9a81)
6512ae7c9f36206f6433f78296102419	Trojan (0055a98e1)

MITRE ATT&CK

Execution	Scheduled Task (T1053)
Service Execution (T1035)	
Command-Line Interface (T1059)	
Persistence	Registry Run Key / Startup Folder (T1060)
Hidden Files and Directories (T1158)	
New Service (T1050)	
Privilege Escalation	Bypass User Account Control (T1088)
Defensive Evasion	Bypass User Account Control (T1088)
Disabling Security Tools (T1089)	
File and Hidden Files and Directories (T1158)	
File Deletion (T1107)	
Process Injection (T1055)	
Modify Registry (T1112)	
Discovery	System Owner/User Discovery (T1033)
Security Software Discovery (T1063)	
Lateral Movement	Exploitation of Remote Services (T1210)