# Chafer: Latest Attacks Reveal Heightened Ambitions

symantec-blogs.broadcom.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

Threat Hunter TeamSymantec

## How Chafer infects targets

In the earlier attacks from 2015, Symantec found evidence that Chafer had been compromising targeted organizations by attacking their web servers, likely through SQL injection attacks, in order to drop malware onto them. In 2017, the group added a new infection method to its toolkit, using malicious documents which are likely circulated using spear-phishing emails sent to individuals working in targeted organizations.

These documents were Excel spreadsheets. When opened, they downloaded a malicious VBS file that in turn ran a PowerShell script. Several hours later, a dropper would appear on the compromised computer. This would install three files on the computer, an information stealer, a screen capture utility, and an empty executable.

The screen capture utility appeared to be used for initial information gathering, as it was only used briefly at the beginning of each infection and not seen again. The information stealer was capable of stealing the contents of the clipboard, taking screenshots, recording keystrokes and stealing files and user credentials. After this initial activity, the attackers usually downloaded more of their tools to the computer using a PowerShell downloader and began moving across the victim's network.

## New tools used to compromise networks

Symantec has seen Chafer use seven new tools in its more recent campaigns, in addition to malware it is previously known to have used. Most of the new tools are freely available, off-the-shelf tools, put to a malicious use. The new tools include:

- **Remcom**: An open-source alternative to PsExec, which is a Microsoft Sysinternals tool used for executing processes on other systems.
- **Non-sucking Service Manager (NSSM**): An open-source alternative to the Windows Service Manager which can be used to install and remove services and will restart services if they crash.
- **A custom screenshot and clipboard capture tool.**
- **SMB hacking tools**: Used in conjunction with other tools to traverse target networks. These tools include the EternalBlue exploit (which was previously used by WannaCry and Petya).
- **GNU HTTPTunnel**: An open-source tool that can create a bidirectional HTTP tunnel on Linux computers, potentially allowing communication beyond a restrictive firewall.
- **UltraVNC**: An open-source remote administration tool for Microsoft Windows.
- **NBTScan**: A free tool for scanning IP networks for NetBIOS name information.

Chafer has also continued to use tools previously associated with the group, including its own custom backdoor Remexi (Backdoor.Remexi); the aforementioned PsExec; Mimikatz (Hacktool.Mimikatz), a free tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext; Pwdump (Pwdump) a tool that is used to grab Windows password hashes from a remote Windows computer; and Plink (PuTTY Link) a command-line utility used to create reverse SSH sessions.

Chafer has used these tools in concert to traverse targeted networks. The group has recently adopted NSSM to maintain persistence and install the service which runs Plink on the compromised computer. Plink is then used to open reverse SSH sessions from the attacker's server to the RDP port on the victim computer. This presumably gives them RDP access to the compromised computer.

Once a foothold is established, the attackers use PsExec, Remcom, and SMB hacking tools to begin moving across the victim's network.

## New infrastructure in use

Chafer has also begun using new infrastructure. The domain win7-updates[.]com is being used by the group as a command and control address. The domain has been referenced several times in command lines, e.g:

- s224.win7-update[.]com
- s5060.win7-update[.]com
- s21.win7-update[.]com

It has also been embedded in a dropper:

hxxp://wsus65432.win7-update[.]com

Symantec also discovered multiple IP addresses that were used as infrastructure by the attackers. It is unclear whether these were leased or hijacked, but the fact that many of them appear to follow a pattern—with the latter three numbers of each address often running in sequence—makes it likely they were deliberately selected by the attackers.

- 107.191.62[.]45
- 94.100.21[.]213
- 89.38.97[.]112
- 148.251.197[.]113
- 83.142.230[.]113
- 87.117.204[.]113
- 89.38.97[.]115
- 87.117.204[.]115
- 185.22.172[.]40
- 92.243.95[.]203
- 91.218.114[.]204
- 86.105.227[.]224
- 91.218.114[.]225
- 134.119.217[.]84

In one case, Symantec found what appeared to be a staging server used by the attackers. The server belonged to one of the targeted organizations. Copies of many of the tools used by the group were discovered on the server. The attackers didn't even bother hiding their activity and saved items to the desktop, often without renaming them.

## Links to Crambus?

Chafer's activities have some links to another group known as Crambus (aka Oilrig). Both groups have been observed using the same IP address for command and control purposes. In addition to this, both groups have been seen using a similar infection vector, namely an

Excel document which drops a malicious VBS file. Both VBS files reference the same file path, containing the same misspelling:

> “schtasks.exe /create/ F /sc minute /mo 2 /tn "UpdatMachine" /tr %LOCALAPPDATA%\microsoft\Feed\Y658123.vbs”

Are the two groups one and the same? While this may be a possibility, at present there isn’t enough evidence to support that hypothesis. What is more likely is that the two groups are known to each other and enjoy access to a shared pool of resources.

## Growing threat to organizations in the Middle East

Chafer’s recent activities indicate that the group remains highly active, is continuing to hone its tools and tactics, and has become more audacious in its choice of targets. Although a regional actor, the group has followed two trends seen globally among targeted attack groups. The first is a greater reliance on freely available software tools, also known as “living off the land.” By limiting their use of malware, groups such as Chafer hope to be less conspicuous on a victim’s network and, if discovered, make their attack more difficult to attribute.

The second trend is towards attacks on the supply chain, compromising organizations with the goal of then attacking the customers, or even the customers of the customers, of those organizations. These attacks require more “steps” to reach their ultimate target, which adds additional time and risk for attackers to reach their targets.  However these attacks also leverage trusted channels into the eventual target, e.g., through a trusted supplier, allowing attackers to potentially circumvent security systems at the organization they ultimately wish to compromise. These attacks are riskier but come with a potentially higher reward and, if successful, could give the attackers access to a vast pool of potential targets.

## About the Author

### Threat Hunter Team

#### Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.