Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments

symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

Symantec DeepSight Adversary Intelligence TeamManaged Adversary and Threat Intelligence (MATI)

Network Protection Security Labs

Waterbug may have hijacked a separate espionage group's infrastructure during one attack against a Middle Eastern target.

The Waterbug espionage group (aka Turla) has continued to attack governments and international organizations over the past eighteen months in a series of campaigns that have featured a rapidly evolving toolset and, in one notable instance, the apparent hijacking of another espionage group's infrastructure.

Three waves of attacks

Recent Waterbug activity can be divided into three distinct campaigns, characterized by differing toolsets. One campaign involved a new and previously unseen backdoor called Neptun (Backdoor.Whisperer). Neptun is installed on Microsoft Exchange servers and is designed to passively listen for commands from the attackers. This passive listening capability makes the malware more difficult to detect. Neptun is also able to download additional tools, upload stolen files, and execute shell commands. One attack during this campaign involved the use of infrastructure belonging to another espionage group known as Crambus (aka OilRig, APT34).

A second campaign used Meterpreter, a publicly available backdoor along with two custom loaders, a custom backdoor called photobased.dll, and a custom Remote Procedure Call (RPC) backdoor. Waterbug has been using Meterpreter since at least early 2018 and, in this campaign, used a modified version of Meterpreter, which was encoded and given a .wav extension in order to disguise its true purpose.

The third campaign deployed a different custom RPC backdoor to that used in the second campaign. This backdoor used code derived from the publicly available PowerShellRunner tool to execute PowerShell scripts without using powershell.exe. This tool is designed to bypass detection aimed at identifying malicious PowerShell usage. Prior to execution, the PowerShell scripts were stored Base64-encoded in the registry. This was probably done to avoid them being written to the file system.

Figure 1. Waterbug group rolls out fresh toolset in three new campaigns

Retooled

Waterbug's most recent campaigns have involved a swath of new tools including custom malware, modified versions of publicly available hacking tools, and legitimate administration tools. The group has also followed the current shift towards "living off the land," making use of PowerShell scripts and PsExec, a Microsoft Sysinternals tool used for executing processes on other systems.

Aside from new tools already mentioned above, Waterbug has also deployed:

- A new custom dropper typically used to install Neptun as a service.
- A custom hacking tool that combines four leaked Equation Group tools (EternalBlue, EternalRomance, DoublePulsar, SMBTouch) into a single executable.
- A USB data collecting tool that checks for a connected USB drive and steals certain file types, encrypting them into a RAR file. It then uses WebDAV to upload to a Box cloud drive.
- Visual Basic scripts that perform system reconnaissance after initial infection and then send information to Waterbug command and control (C&C) servers.
- PowerShell scripts that perform system reconnaissance and credential theft from Windows Credential Manager and then send this information back to Waterbug C&Cs.
- Publicly available tools such as IntelliAdmin to execute RPC commands, SScan and NBTScan for network reconnaissance, PsExec for execution and lateral movement, and Mimikatz (Hacktool.Mimikatz) for credential theft, and Certutil.exe to download and decode remote files. These tools were identified being downloaded via Waterbug tools or infrastructure.

Victims

These three recent Waterbug campaigns have seen the group compromise governments and international organizations across the globe in addition to targets in the IT and education sectors. Since early 2018, Waterbug has attacked 13 organizations across 10 different countries:

- The Ministry of Foreign Affairs of a Latin American country
- The Ministry of Foreign Affairs of a Middle Eastern country
- The Ministry of Foreign Affairs of a European country
- The Ministry of the Interior of a South Asian country
- Two unidentified government organizations in a Middle Eastern country
- One unidentified government organization in a Southeast Asian country
- A government office of a South Asian country based in another country
- An information and communications technology organization in a Middle Eastern country

- Two information and communications technology organizations in two European countries
- An information and communications technology organization in a South Asian country
- A multinational organization in a Middle Eastern country
- An educational institution in a South Asian country

Hijacked infrastructure

One of the most interesting things to occur during one of Waterbug's recent campaigns was that during an attack against one target in the Middle East, Waterbug appeared to hijack infrastructure from the Crambus espionage group and used it to deliver malware on to the victim's network. Press reports have linked Crambus and Waterbug to different nation states. While it is possible that the two groups may have been collaborating, Symantec has found no further evidence to support this. In all likelihood, Waterbug's use of Crambus infrastructure appears to have been a hostile takeover. Curiously though, Waterbug also compromised other computers on the victim's network using its own infrastructure.

During this attack, a customized variant of the publicly available hacking tool Mimikatz was downloaded to a computer on the victim's network from known Crambus-controlled network infrastructure. Mimikatz was downloaded via the Powruner tool and the Poison Frog control panel. Both the infrastructure and the Powruner tool have been publicly tied to Crambus by a number of vendors. Both were also mentioned in recent leaks of documents tied to Crambus.

Symantec believes that the variant of Mimikatz used in this attack is unique to Waterbug. It was heavily modified, with almost all original code stripped out aside from its sekurlsa::logonpasswords credential stealing feature. Waterbug has frequently made extensive modifications to publicly available tools, something Crambus is not well known for.

The variant of Mimikatz used was packed with a custom packing routine that has not been seen before in any non-Waterbug malware. Waterbug used this same packer on a second custom variant of Mimikatz and on a dropper for the group's custom Neuron service (Trojan.Cadanif). Its use in the dropper leads us to conclude that this custom packer is exclusively used by Waterbug. Additionally, this version of Mimikatz was compiled using Visual Studio and the publicly available bzip2 library which, although not unique, has been used by other Waterbug tools previously.

Aside from the attack involving Crambus infrastructure, this sample of Mimikatz has only been seen used in one other attack, against an education target in the UK in 2017. On that occasion, Mimikatz was dropped by a known Waterbug tool.

In the case of the attack against the Middle Eastern target, Crambus was the first group to compromise the victim's network, with the earliest evidence of activity dating to November 2017. The first observed evidence of Waterbug activity came on January 11, 2018, when a Waterbug-linked tool (a task scheduler named msfgi.exe) was dropped on to a computer on

the victim's network. The next day, January 12, the aforementioned variant of Mimikatz was downloaded to the same computer from a known Crambus C&C server. Two further computers on the victim's network were compromised with Waterbug tools on January 12, but there is no evidence that Crambus infrastructure was used in these attacks. While one of these computers had been previously compromised by Crambus, the other showed no signs of Crambus intrusion.

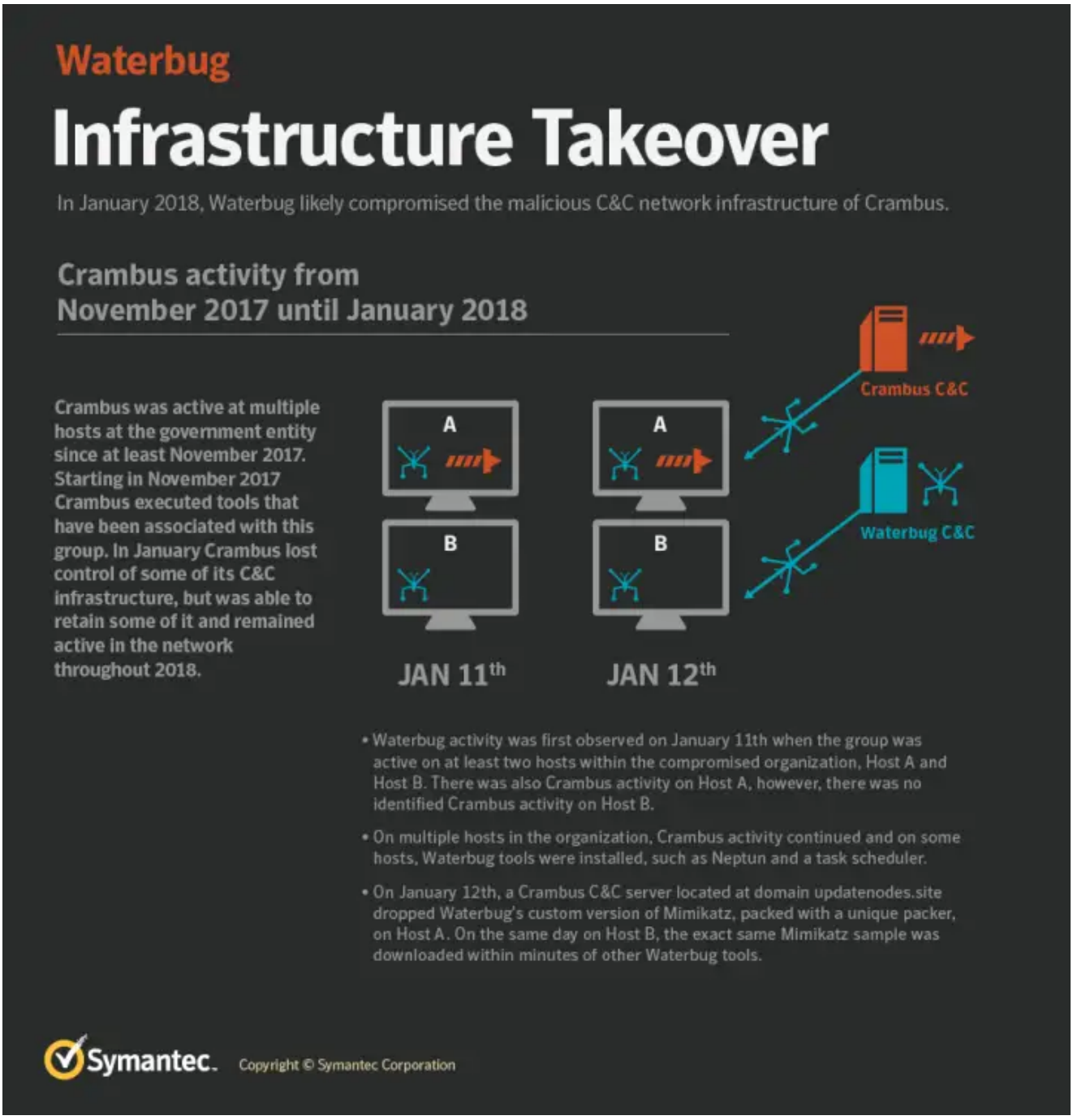

Figure 2. Waterbug likely compromised the C&C network infrastructure of Crambus

Waterbug's intrusions on the victim's network continued for much of 2018. On September 5, 2018, a similar Mimikatz variant was dropped by Waterbug's Neptun backdoor onto another computer on the network. At around the same time, other Waterbug malware was seen on the victim's network which communicated with known Waterbug C&C servers.

Finally, the issue was clouded further by the appearance of a legitimate systems administration tool called IntelliAdmin on the victim's network. This tool is known to have been used by Crambus and was mentioned in the leak of Crambus documents. However, in this case, IntelliAdmin was dropped by custom Waterbug backdoors, including the newly identified Neptun backdoor, on computers that had not been affected by the Crambus compromise.

The incident leaves many unanswered questions, chiefly relating to Waterbug's motive for using Crambus infrastructure. There are several possibilities:

1. **False flag**: Waterbug does have a track record of using false flag tactics to throw investigators off the scent. However, if this was a genuine attempt at a false flag operation, it begs the question of why it also used its own infrastructure to communicate with other machines on the victim's network, in addition to using tools that could be traced back to Waterbug.
2. **Means of intrusion:** It is possible that Waterbug wanted to compromise the target organization, found out that Crambus had already compromised its network, and hijacked Crambus's own infrastructure as a means of gaining access. Symantec did not observe the initial access point and the close timeframe between Waterbug observed activity on the victim's network and its observed use of Crambus infrastructure suggests that Waterbug may have used the Crambus infrastructure as an initial access point.
3. **Mimikatz variant belonged to Crambus:** There is a possibility that the version of Mimikatz downloaded by the Crambus infrastructure was actually developed by Crambus. However, the compilation technique and the fact that the only other occasion it was used was linked to Waterbug works against this hypothesis. The fact that Waterbug also appeared on the victim's network around the same time this version of Mimikatz was downloaded would make it an unlikely coincidence if the tool did belong to Crambus.
4. **Opportunistic sowing of confusion:** If a false flag operation wasn't planned from the start, it is possible that Waterbug discovered the Crambus intrusion while preparing its attack and opportunistically used it in the hopes of sowing some confusion in the mind of the victim or investigators. Based on recent leaks of Crambus internal documents, its Poison Frog control panel is known to be vulnerable to compromise, meaning it may have been a relatively trivial diversion on the part of Waterbug to hijack Crambus's infrastructure. A compromise conducted by one threat actor group through another's infrastructure, or fourth party collections, has been previously discussed in a 2017 white paper by Kaspersky researchers.

Further campaigns

Waterbug has also mounted two other campaigns over the past year, each of which was characterized by separate tools. These campaigns were wide ranging, hitting targets in Europe, Latin America, and South Asia.

In the first campaign, Waterbug used two versions of a custom loader named javavs.exe (64-bit) and javaws.exe (32-bit), to load a custom backdoor named PhotoBased.dll and run the export function GetUpdate on the victim's computers. The backdoor will modify the registry for the Windows Media Player to store its C&C configuration. It also reconfigures the Microsoft Sysinternals registry to prevent pop-ups when running the PsExec tool. The backdoor has the capability to download and upload files, execute shell commands, and update its configuration.

The javaws.exe loader is also used to run another loader named tasklistw.exe. This is used by the attackers to decode and execute a series of malicious executables that download Meterpreter to the infected computer.

The attackers also install another backdoor that runs a command shell via the named pipe cmd_pipe. Both backdoors allow the attackers to execute various commands that provide full control of the victim's system. Waterbug also used an older version of PowerShell, likely to avoid logging.

In the second campaign, Waterbug used an entirely different backdoor, named securlsa.chk. This backdoor can receive commands through the RPC protocol. Its capabilities include:

- Executing commands through cmd.exe with the output redirected into a temporary file
- Reading the command output contained in the temporary file
- Reading or writing arbitrary files

This RPC backdoor also included source code derived from the tool PowerShellRunner, which allows a user to run PowerShell scripts without executing powershell.exe, therefore the user may bypass detection aimed at identifying malicious PowerShell usage.

While both campaigns involved distinct tools during the initial compromise phase, there were also many similarities. Both were characterized by the use of a combination of custom malware and publicly available tools. Also, during both campaigns Waterbug executed multiple payloads nearly simultaneously, most likely to ensure overlapping access to the network if defenders found and removed one of the backdoors.

Waterbug took several steps to avoid detection. It named Meterpreter as a WAV file type, probably in the hope that this would not raise suspicions. The group also used GitHub as a repository for tools that it downloaded post-compromise. This too was likely motivated by a desire to evade detection, since GitHub is a widely trusted website. It used Certutil.exe to download files from the repository, which is an application whitelist bypass technique for remote downloads.

In one of these campaigns, Waterbug used a USB stealer that scans removable storage devices to identify and collect files of interest. It then packages stolen files into a password-protected RAR archive. The malware then uses WebDAV to upload the RAR archive to a Box account.

Unanswered questions

This is the first time Symantec has observed one targeted attack group seemingly hijack and use the infrastructure of another group. However, it is still difficult to ascertain the motive behind the attack. Whether Waterbug simply seized the opportunity to create confusion about the attack or whether there was more strategic thinking involved remains unknown.

Waterbug's ever-changing toolset demonstrates a high degree of adaptability by a group determined to avoid detection by staying one step ahead of its targets. Frequent retooling and a penchant for flirting with false flag tactics have made this group one of the most challenging adversaries on the targeted attack landscape.

Protection/Mitigation

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Backdoor.Whisperer
- Hacktool.Mimikatz

Threat Intelligence

The DeepSight Managed Adversary and Threat Intelligence (MATI) team co-authored this blog and its customers have received intelligence with additional details about these campaigns, the characteristics of the Waterbug (aka Turla) cyber espionage group, and methods of detecting and thwarting activities of this adversary.

Indicators of Compromise

Campaign 1

- 24fe571f3066045497b1d8316040734c81c71dcb1747f1d7026cda810085fad7
- 66893ab83a7d4e298720da28cd2ea4a860371ae938cdd86035ce920b933c9d85
- 7942eee31d8cb1c8853ce679f686ee104d359023645c7cb808361df791337145
- 7bd3ff9ba43020688acaa05ce4e0a8f92f53d9d9264053255a5937cbd7a5465e
- a1d9f5b9ca7dda631f30bd1220026fc8c3a554d61db09b5030b8eb9d33dc9356
- c63f425d96365d906604b1529611eefe5524432545a7977ebe2ac8c79f90ad7e
- cb7ecd6805b12fdb442faa8f61f6a2ee69b8731326a646ba1e8886f0a5dd61e0
- db9902cb42f6dc9f1c02bd3413ab3969d345eb6b0660bd8356a0c328f1ec0c07

- e0c316b1d9d3d9ec5a97707a0f954240bbc9748b969f9792c472d0a40ab919ea
- e0c316b1d9d3d9ec5a97707a0f954240bbc9748b969f9792c472d0a40ab919ea
- 5da013a64fd60913b5cb94e85fc64624d0339e09d7dce25ab9be082f0ca5e38b
- c8a864039f4d271f4ab6f440cbc14dffd8c459aa3af86f79f0619a13f67c309f
- 588fd8eba6e62c28a584781deefe512659f6665daeb8c85100e0bf7a472ad825
- cda5b20712e59a6ba486e55a6ab428b9c45eb8d419e25f555ae4a7b537fc2f26
- 694d9c8a1f0563c08e0d3ab7d402ffbf5a0fa11340c50fba84d709384ccef021
- caaed70daa7832952ae93f41131e74dcb6724bb8669d18f28fbed4aa983fdc0c
- 493eee2c55810201557ef0e5d134ca0d9569f25ae732df139bb0cb3d1478257f
- 0e9c3779fece579bed30cb0b7093a962d5de84faa2d72e4230218d4a75ee82bc
- 5bbeed53aaa40605aabbfde31cbfafd5b92b52720e05fa6469ce1502169177a0
- d153e4b8a11e2537ecf99aec020da5fad1e34bbe79f617a3ee5bc0b07c3abdca

- vision2030.tk
- vision2030.cf
- dubaiexpo2020.cf
- microsoft.updatemeltdownkb7234.com
- codewizard.ml
- updatenodes.site

- https://vision2030.tk/static/googleupdate.txt
- https://dubaiexpo2020.cf/counter.aspx
- https://microsoft.updatemeltdownkb7234.com/windows/update.aspx
- https://codewizard.ml/productivity/update.aspx

Campaign 2

- 10d1bfd5e8e1c8fa75756a9f1787c3179da9ab338a476f1991d9e300c6186575
- 3fbec774da2a145974a917aeb64fc389345feb3e581b46d018077e28333601a5
- 52169d7cdd01098efdde4da3fb22991aaa53ab9e02db5d80114a639bf65bce39
- 56098ed50e25f28d466be78a36c643d19fedc563a2250ae86a6d936318b7f57e
- 595a54f0bbf297041ce259461ae8a12f37fb29e5180705eafb3668b4a491cecc
- 5dc26566b4dec09865ea89edd4f9765ef93e789870ed4c25fcc4ebad19780b40
- 6b60b27385738cac65584cf7d486913ff997c66d97a94e1dde158c9cd03a4206
- 846a95a26aac843d1fcec51b2b730e9e8f40032ee4f769035966169d68d144c4
- c4a6db706c59a5a0a29368f80731904cc98a26e081088e5793764a381708b1ea
- d0b99353cb6500bb18f6e83fe9eed9ce16e5a8d5b940181e5eafd8d82f328a59
- ee7f92a158940a0b5d9b902eb0ed9a655c7e6ba312473b1e2c9ef80d58baa6dd

  94.249.192.182

Campaign 3

- 454e6c3d8c1c982cd301b4dd82ec3431935c28adea78ed8160d731ab0bed6cb7

- 4ecb587ee9b872747408c00de5619cb6b973e7d39ce4937655c5d1a07b7500fc
- 528e2567e24809d2d0ba96fd70e41d71c18152f0f0c4f29ced129ed7701fa42a
- 6928e212874686d29c85eac72553ccdf89aacb475c61fa3c086c796df3ab5940
- b22bbda8f504f8cced886f566f954cc245f3e7c205e57139610bbbff0412611c
- d52b08dd27f2649bad764152dfc2a7dea0c8894ce7c20b51482f4a4cf3e1e792
- e7e41b3d7c0ee2d0939bb56d797eaf2dec44516ba54b8bf1477414b03d4d6e48
- ec3da59d4a35941f6951639d81d1c5ff73057d9cf779428d80474e9656db427c
- fbefe503d78104e04625a511528584327ac129c3436e4df09f3d167e438a1862

- markham-travel.com
- zebra.wikaba.com
- 185.141.62.32
- 212.21.52.110

Threat Intelligence5 Min Read

Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms

Group remains highly active with more than 130 victims in 30 organizations hit since September 2018.

About the Author

Symantec DeepSight Adversary Intelligence Team

Managed Adversary and Threat Intelligence (MATI)

Symantec's managed adversary and threat intelligence (MATI) team of intelligence analysts & researchers are dedicated to understanding the adversary ecosystem and providing insightful customer reports detailing their plans, tactics, tools, and campaigns.

About the Author

Network Protection Security Labs

Network Protection Security Labs is a group of security experts within Network Protection Products doing advanced security research to continuously improve Symantec Network Products.

Want to comment on this post?