Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak

symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

Key Findings

- The Buckeye attack group was using Equation Group tools to gain persistent access to target organizations at least a year prior to the Shadow Brokers leak.
- Variants of Equation Group tools used by Buckeye appear to be different from those released by Shadow Brokers, potentially indicating a different origin.
- Buckeye's use of Equation Group tools also involved the exploit of a previously unknown Windows zero-day vulnerability. This zero day was reported by Symantec to Microsoft in September 2018 and patched in March 2019.
- While Buckeye appeared to cease operations in mid-2017, the Equation Group tools it used continued to be used in attacks until late 2018. It is unknown who continued to use the tools. They may have been passed to another group or Buckeye may have continued operating longer than supposed.

The 2017 leak of Equation Group tools by a mysterious group calling itself the Shadow Brokers was one of the most significant cyber security stories in recent years. Equation is regarded as one of the most technically adept espionage groups and the release of a trove of its tools had a major impact, with many attackers rushing to deploy the malware and exploits disclosed. One of these tools, the EternalBlue exploit, was used to devastating effect in the May 2017 WannaCry ransomware outbreak.

However, Symantec has now found evidence that the Buckeye cyber espionage group (aka APT3, Gothic Panda) began using Equation Group tools in attacks at least a year prior to the Shadow Brokers leak.

Beginning in March 2016, Buckeye began using a variant of DoublePulsar (Backdoor.Doublepulsar), a backdoor that was subsequently released by the Shadow Brokers in 2017. DoublePulsar was delivered to victims using a custom exploit tool (Trojan.Bemstour) that was specifically designed to install DoublePulsar.

Bemstour exploits two Windows vulnerabilities in order to achieve remote kernel code execution on targeted computers. One vulnerability is a Windows zero-day vulnerability (CVE-2019-0703) discovered by Symantec. The second Windows vulnerability (CVE-2017-0143) was patched in March 2017 after it was discovered to have been used by two exploit tools—EternalRomance and EternalSynergy—that were also released as part of the Shadow Brokers leak.

The zero-day vulnerability allows for the leaking of information and can be exploited in conjunction with other vulnerabilities to attain remote kernel code execution. It was reported by Symantec to Microsoft in September 2018 and was patched on March 12, 2019.

How Buckeye obtained Equation Group tools at least a year prior to the Shadow Brokers leak remains unknown.

Buckeye disappeared in mid-2017 and three alleged members of the group were indicted in the U.S. in November 2017. However, while activity involving known Buckeye tools ceased in mid-2017, the Bemstour exploit tool and the DoublePulsar variant used by Buckeye continued to be used until at least September 2018 in conjunction with different malware.

History of attacks

The Buckeye attack group had been active since at least 2009, when it began mounting a string of espionage attacks, mainly against organizations based in the U.S.

The group has a record of exploiting zero-day vulnerabilities. These include CVE-2010-3962 as part of an attack campaign in 2010 and CVE-2014-1776 in 2014. Although other zero-day attacks have been reported, they have not been confirmed by Symantec. All zero-day exploits known, or suspected, to have been used by this group are for vulnerabilities in Internet Explorer and Flash.

Timeline of attacks

Beginning in August 2016, a group calling itself the Shadow Brokers began releasing tools it claimed to have originated from the Equation Group. It initially released samples of the information it had, offering the full trove to the highest bidder. Over the coming months, it progressively released more tools, until April 2017, when it released a final, large cache of tools, including the DoublePulsar backdoor, the FuzzBunch framework, and the EternalBlue, EternalSynergy, and EternalRomance exploit tools.

However, Buckeye had already been using some of these leaked tools at least a year beforehand. The earliest known use of Equation Group tools by Buckeye is March 31, 2016, during an attack on a target in Hong Kong. During this attack, the Bemstour exploit tool was delivered to victims via known Buckeye malware (Backdoor.Pirpi). One hour later, Bemstour was used against an educational institution in Belgium.

Bemstour is specifically designed to deliver a variant of the DoublePulsar backdoor. DoublePulsar is then used to inject a secondary payload, which runs in memory only. The secondary payload enables the attackers to access the affected computer even after DoublePulsar is removed. It is worth noting that earlier versions did not include any means of uninstalling the DoublePulsar implant. This functionality was added in later versions.

A significantly improved variant of the Bemstour exploit tool was rolled out in September 2016, when it was used in an attack against an educational institution in Hong Kong. While the original variant was only capable of exploiting 32-bit systems, the new variant could exploit both 32-bit and 64-bit targets, adding support for newer Windows versions. Another new feature of the payload in the second variant allowed the attacker to execute arbitrary shell commands on the infected computer. This custom payload is also designed to copy arbitrary files and execute arbitrary processes on the targeted computer. When used against 32-bit targets, Bemstour still delivered the same DoublePulsar backdoor. However, against 64-bit targets it delivered only the custom payload. The attackers typically used it to execute shell commands that created new user accounts.

Bemstour was used again in June 2017 in an attack against an organization in Luxembourg. Unlike earlier attacks when Bemstour was delivered using Buckeye's Pirpi backdoor, in this attack Bemstour was delivered to the victim by a different backdoor Trojan (Backdoor.Filensfer). Between June and September 2017, Bemstour was also used against targets in the Philippines and Vietnam.

Development of Bemstour has continued into 2019. The most recent sample of Bemstour seen by Symantec appears to have been compiled on March 23, 2019, eleven days after the zero-day vulnerability was patched by Microsoft.

The purpose of all the attacks was to acquire a persistent presence on the victim's network, meaning information theft was the most likely motive of the attacks.

Target locations	Hong Kong, Belgium	Hong Kong	Luxembourg	Philippines	Vietnam

Tools	Back-door.Pirpi	Unknown		Back-door.-Filensfer	Unknown	Unknown
	Bemstour Exploit Tool (V1)	Bemstour Exploit Tool (V2)	Shadow Brokers Leak	Bemstour Exploit Tool (V1)	Bemstour Exploit Tool (V1 & V2)	Bemstour Exploit Tool (V2)
	Double-Pulsar	DoublePulsar (32-bit) or custom payload only (64-bit)		Double-Pulsar	DoublePulsar (32-bit) or custom payload only (64-bit)	DoublePulsar (32-bit) or custom payload only (64-bit)

Table 1. Buckeye Tool Usage Over Time

The Filensfer connection

Filensfer is a family of malware that has been used in targeted attacks since at least 2013. Symantec has found multiple versions of the malware, including a C++ version, a compiled Python version (using py2exe), and a PowerShell version.

Over the past three years, Filensfer has been deployed against organizations in Luxembourg, Sweden, Italy, the UK, and the U.S. Targets included organizations in the telecoms, media, and manufacturing sectors. While Symantec has never observed the use of Filensfer alongside any known Buckeye tools, information shared privately by another vendor included evidence of Filensfer being used in conjunction with known Buckeye malware (Backdoor.Pirpi).

Bemstour exploit tool

Bemstour exploits two Windows vulnerabilities in order to achieve remote kernel code execution on targeted computers.

The zero-day vulnerability found and reported by Symantec (CVE-2019-0703) occurs due to the way the Windows SMB Server handles certain requests. The vulnerability allows for the leaking of information.

The second vulnerability (CVE-2017-0143) is a message type confusion vulnerability. When the two vulnerabilities are exploited together, the attacker can gain full access in the form of kernel mode code execution, enabling them to deliver malware to the targeted computer.

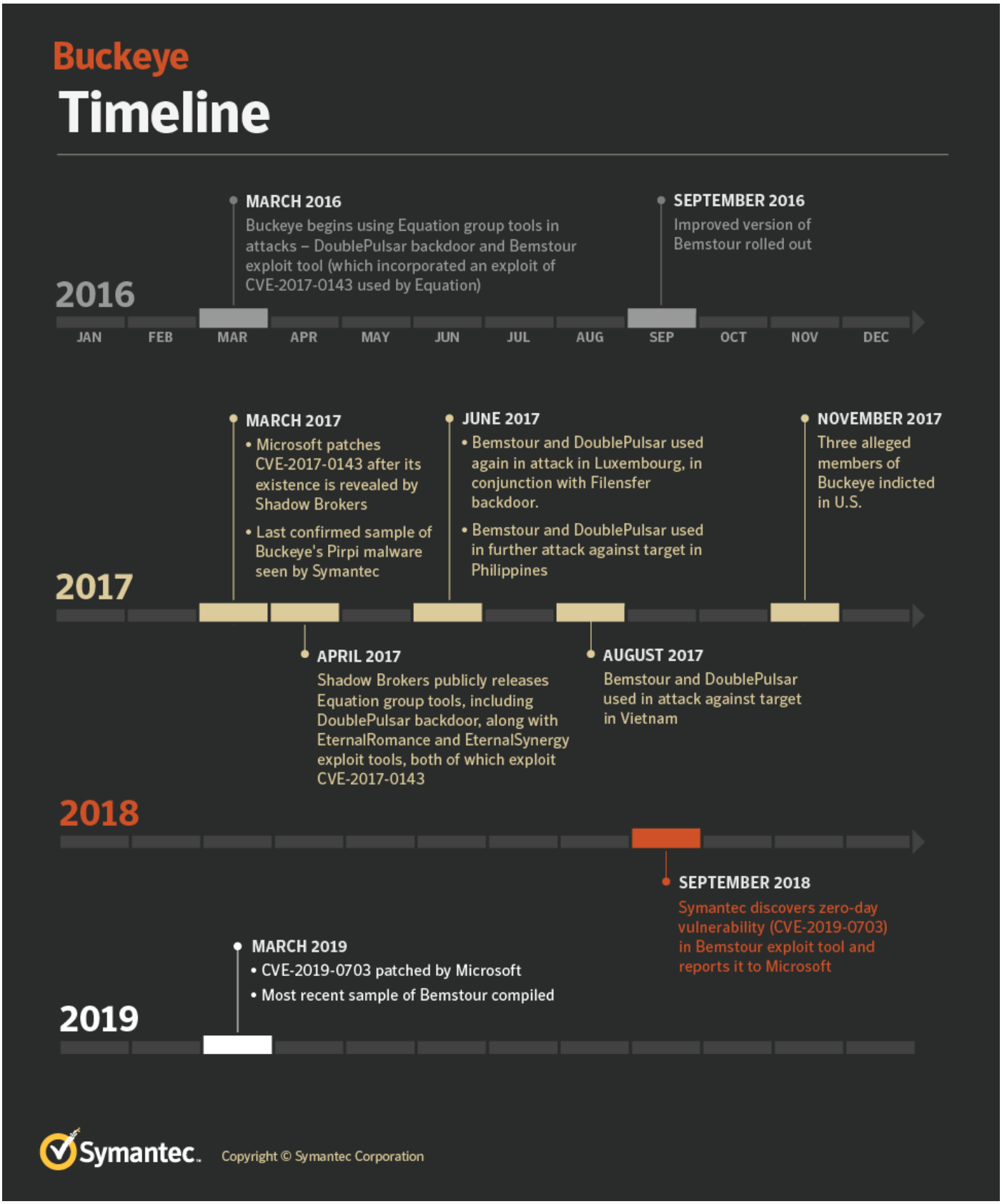
When Bemstour was first used in 2016, both vulnerabilities were zero days, although CVE-2017-0143 was subsequently patched by Microsoft in March 2017 (MS17-010). CVE-2017-0143 was also used by two other exploit tools—EternalRomance and EternalSynergy—that were released as part of the Shadow Brokers leak in April 2017.

Buckeye's exploit tool, EternalRomance, as well as EternalSynergy, can exploit the CVE-2017-0143 message type confusion vulnerability to perform memory corruption on unpatched victim computers. In order to obtain remote code execution capabilities, all three exploit tools needed to collect information about the memory layout of attacked systems in addition to exploiting the aforementioned message type confusion vulnerability. Each tool performed this differently, relying on different vulnerabilities. In the case of the Buckeye exploit tool, the attackers exploited their own zero-day vulnerability (CVE-2019-0703).

DoublePulsar development

The variant of DoublePulsar used in the first attacks performed by Buckeye was different to that leaked by the Shadow Brokers. It appears to contain code to target newer versions of Windows (Windows 8.1 and Windows Server 2012 R2), indicating that it is a newer version of the malware. It also includes an additional layer of obfuscation. Based on technical features and timing, it is possible that this obfuscation was created by DoublePulsar's original authors.

It is noteworthy that the attackers never used the FuzzBunch framework in its attacks. FuzzBunch is a framework designed to manage DoublePulsar and other Equation Group tools and was leaked by the Shadow Brokers in 2017. This suggests that Buckeye only managed to gain access to a limited number of Equation Group tools.



Unanswered questions

There are multiple possibilities as to how Buckeye obtained Equation Group tools before the Shadow Brokers leak. Based on the timing of the attacks and the features of the tools and how they are constructed, one possibility is that Buckeye may have engineered its own version of the tools from artefacts found in captured network traffic, possibly from observing an Equation Group attack. Other less supported

scenarios, given the technical evidence available, include Buckeye obtaining the tools by gaining access to an unsecured or poorly secured Equation Group server, or that a rogue Equation group member or associate leaked the tools to Buckeye.

Mystery also surrounds the continued use of the exploit tool and DoublePulsar after Buckeye's apparent disappearance. It may suggest that Buckeye retooled following its exposure in 2017, abandoning all tools publicly associated with the group. However, aside from the continued use of the tools, Symantec has found no other evidence suggesting Buckeye has retooled. Another possibility is that Buckeye passed on some of its tools to an associated group.

Protection

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

File-based protection

Network protection products

Indicators of Compromise

7020bcb347404654e17f6303848b7ec4	cbe23daa9d2f8e1f5d59c8336d-d5b7d7ba1d5cf3f0d45e66107668e80b073ac3	Pirpi (first variant)
aacfef51a4a242f52fbb838c1d063d9b	53145f374299e673d82d108b133341d-c7bee642530b560118e3cbcdb981ee92c	Pirpi (second variant)
c2f902f398783922a921df7d46590295	01f53953d-b8ba580ee606043a482f790082460c8cdbd7f-f151d84e03fdc87e42	Command line utility to list user accounts on remote machine
6458806a5071a7c4fefae084791e8c67	6b1f8b303956c04e24448b1eec8634bd3f-b2784c8a2d12ecf8588424b36d3cbc	Filensfer (C/C++)
0d2d0d8f4989679f7c26b5531096b8b2	7b-fad342ce88de19d090a4cb2ce332022650ab-d68f34e83fdc694f10a4090d65	Filensfer (Powershell)
a3932533efc04ac3fe89fb5b3d60128a	3dbe8700ecd27b3dc39643b95b187c-cfd44318fc88c5e6ee6acf3a07cdaf377e	Filensfer (py2exe)
58f784c7a292103251930360f9ca713e	1c9f1c7056864b5fdd491d5-daa49f920c3388cb8a8e462b2bc34181ce-f6c1f9c	Command line SMB client
a469d48e25e524cf0dec64f01c182b25	951f079031c996c85240831ea1b61507f91990282daae6da2841311322e8a6d7	HTran

Threat intelligence

In addition to file-based protection, customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received reports on Buckeye, which detail methods of detecting and thwarting activities of this group.