Booz | Allen | Hamilton

BOOZ ALLEN CYBER4SIGHT

JULY 12, 2017

Telebots Group may have used PETYA variant to destroy evidence of long-term campaign.

The Booz Allen Cyber4Sight® threat intelligence solutions team investigated the Script2Exe-compiled TeleBots backdoors identified by ESET researchers[1] and **identified evidence that suggests that the TeleBots actors may have compromised the MEDoc update service with the goal of performing more traditional intrusion activities across multiple organizations.**

Booz Allen Cyber4Sight assesses that the actors may have then used the Petya malware variant (aka NotPetya, exPetr, Petrwrap, Goldeneye, Nyetya) as a mechanism for wiping forensic evidence of their activities at the conclusion of the campaign. This assessment is derived from the following evidence:

1. Four VirusTotal users uploaded the compiled VBS backdoors along with other malicious files, including the TeleBots telegram-based backdoor, PowerShell post-exploitation scripts, Mimikatz, and other tools. For each user, these uploads occurred within the same one- to two-day time period.
2. In most cases, these files were uploaded several months prior to the 27 June Petya incident.
3. Booz Allen Cyber4Sight also determined that in several cases, these submitters also uploaded files associated with the MEDoc update utility to VirusTotal. This shows that these submitters were also likely users of the MEDoc software, and the inclusion of these files with the files identified in number 1 (above) demonstrates that MEDoc-related processes may have facilitated the installation vector for this software.

TECHNICAL INFORMATION

Booz Allen Cyber4Sight identified four VirusTotal submitters who uploaded the compiled VBS backdoors in within the same one- to two-day time period that they uploaded other files related to post-exploitation activities. In some cases, these files are, according to ESET, uniquely associated with the TeleBots group and include their Telegram-based backdoor. Three of the submitters also uploaded components of the MEDoc software. These three users were also identified on VirusTotal as being located in the Ukraine at the time of the upload. Taken together, this suggests that these three uploads were Ukrainian users of this update utility and may have received intrusive, non-ransomware software via the compromised MEDoc server prior to the Petya attacks. These include:

- **Submitter 1**, who uploaded MEDoc software, the compiled VBS backdoor, a Sysinternals tool, Mimikatz, and the TeleBots Telegram backdoor.
- **Submitter 2**, who uploaded MEDoc software, the compiled VBS backdoor, a separate VBS file connecting to a reported TeleBots C2, a copy of Mimikatz, and a batch file used to execute and save the data from Mimikatz.

[1] https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

- **Submitter 3**, who uploaded MEDoc software, the compiled VBS backdoor, and a PowerShell file containing commands lifted from PowerShell Empire, a post-exploitation suite that Booz Allen Cyber4Sight has previously associated with the TeleBots group.
- **Submitter 4**, who uploaded the compiled VBS backdoor and a copy of psexec. This VirusTotal user is based in the United States and may not be a victim of these attacks.

Booz Allen Cyber4Sight assesses that the TeleBots actors may have used the MEDoc software to deploy their traditional backdoor software and other post-exploitation tools across several organizations in the months prior to the Petya attacks, based on this submission information. At the conclusion of this activity, the actors may have then deployed the malware, which wiped forensic evidence.

Based on data collected from these VirusTotal submissions, Booz Allen Cyber4Sight hypothesizes that the goal of the threat actors in these attacks was not purely destructive, but rather to conduct a more traditional intrusion and collect information from targeted organizations primarily located in the Ukraine. Furthermore, we believe that the ransomware attacks may have been intentionally designed to disguise this true intention. To verify this hypothesis, information from incident response activities demonstrating actual exfiltration of data would need to be made available.

The table of the VirusTotal findings is below. While this table does not contain every file uploaded by these submitters in the March to July 2017 timeframe, Booz Allen Cyber4Sight assesses that these submitters likely represent individual users or individual organizations based on the low volume of submissions per day for each ID. Submission IDs are redacted in this public report; Booz Allen Cyber4Sight customers and trusted partners have received the associated submission IDs.

Date	MD5	File	Notes
Submitter 1 – Ukraine			
May 25th 2017, 06:01:41.000	5761dae7320e40a275fe043a6f8456f6	ezvit.10.01.181-10.01.182.exe.upd	MEDoc-related file
May 25th 2017, 05:59:06.000	1b2a4735c9947ee68c81478c7bc29968	ezvit.10.01.180-10.01.181.exe.upd	MEDoc-related file
May 25th 2017, 05:33:10.000	bcc77ef60faa9855aa2825d5eb3216b7	ezvit.10.01.178-10.01.179.exe.upd	MEDoc-related file
March 23rd 2017, 15:17:11.000	2c581de36790abfeb929e3fafbb17047	$RY0SBR4.exe	Telegram TeleBots Backdoor, connects to api.telegram[.]org
March 23rd 2017, 15:12:29.000	53651050b09b06b0a1c407eb6f6af512	$RWFGSZ7.exe	Mimikatz
March 23rd 2017, 15:10:48.000	c478ca76cd80fe2e82bcb0c40ba00ac8	$RFZGPWO.exe	VBS Backdoor, compiled as an executable
March 23rd 2017, 15:09:53.000	ff9def4ba24e680733c756d2dc60111d	$ROLZ4BF.exe	Sysinternals Access Check
March 23rd 2017, 15:07:33.000	4137dfdf013cb04afbb2df0d8c9ae32f	no recoil-jw.vbs	Old file, may be unrelated to TeleBots activity
Submitter2 – Ukraine			
June 27th 2017, 09:21:02.000	ezvit.10.01.188-10.01.189.exe	a11d0ec8c6ce067967894cf81b8cc610	MEDoc-related file
June 27th 2017, 09:20:11.000	ezvit.10.01.187-10.01.188.exe	bfa32bd387889de0ec0e9554f6ea55ed	MEDoc-related file

Date	MD5	File	Notes
April 27th 2017, 10:47:35.000	e6c0b32c3a3dc4c170d9483804947445	upd.vbs	VBS backdoor, connects to known C2 (hxxps://bankstat.kiev[.]ua)
April 27th 2017, 10:41:38.000	8338c18743f88d813990fe1a973ae12a	spoolsv.exe	VBS backdoor, compiled as an executable
April 27th 2017, 10:40:46.000	60ee11e888ab51dec7179367bdbc395a	1.bat	Z:\Windows\apppatch\Custom\m.exe > Z:\Windows\apppatch\Custom\logms.txt
April 27th 2017, 10:32:15.000	85e025a33578cb77ae0e7cc9ef1590c1	m.exe	Mimikatz
Submitter 3 – Ukraine			
May 22nd 2017, 09:33:58.000	2bd7ebd35266284000a9fbfe4530b9ef	ezvit.10.01.174-10.01.175.exe	MEDoc-related file
May 22nd 2017, 05:39:34.000	cae104b2bf9a5a80e7235e13bd7d26ee	domain.ps1	PowerShell Empire commands
May 22nd 2017, 03:43:01.000	569093e532025471324e2d12ddb1720f	64.rar	
May 22nd 2017, 02:49:04.000	2bd7ebd35266284000a9fbfe4530b9ef	ezvit.10.01.174-10.01.175.exe	MEDoc-related file
May 13th 2017, 07:09:56.000	3d35ce976f6458cccfc2bca998a09621	ezvit.10.01.171-10.01.172.exe	MEDoc-related file
May 13th 2017, 07:08:23.000	f14cf08e0faeaa8153b04181e38bce1c	ezvit.10.01.172-10.01.173.exe	MEDoc-related file
May 13th 2017, 07:06:55.000	37f9fb212065bf4062bbadec6ef0254f	ezvit.10.01.173-10.01.174.exe	MEDoc-related file
May 13th 2017, 07:05:19.000	2bd7ebd35266284000a9fbfe4530b9ef	ezvit.10.01.174-10.01.175.exe	MEDoc-related file
May 13th 2017, 07:01:57.000	fd019a14e6cdf7d15126b774821356d6	ezvit.10.01.175-10.01.176.exe	MEDoc-related file
May 13th 2017, 06:30:25.000	5f4a10fec62f3e75edfe4fb8876402d5	iertutil.dll	
May 13th 2017, 06:05:04.000	8338c18743f88d813990fe1a973ae12a	spoolsv.ex1	VBS backdoor, compiled as an executable
May 12th 2017, 05:47:03.000	8b224e49c97807d60b8646fde9591433	DMF.Native.dll	MEDoc related (per Carbon Black notes in VirusTotal)
May 11th 2017, 09:20:52.000	e4291be333827e843d8db412c29a3e18	UniCryptC.exe	
May 11th 2017, 09:16:43.000	569093e532025471324e2d12ddb1720f	64.rar	
Submitter 4 – United States			

Date	MD5	File	Notes
June 28th 2017, 03:48:36.000	a283e768fa12ef33087f07b01f82d6dd	PSEXESVC.E_XE	psexec
June 28th 2017, 03:46:50.000	aeee996fd3484f28e5cd85fe26b6bdcd	dllhost.dat	psexec
June 27th 2017, 03:44:11.000	33fe357c02c3acdbc6058cb33c841946	smss.e__xe	VBS backdoor, compiled as an executable

About Booz Allen Hamilton

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world.

About Booz Allen Cyber4Sight

Booz Allen Cyber4Sight delivers customers the comfort of knowing that our comprehensive and context-rich threat intelligence enables them with everything they need to prioritize strategic security decisions and to detect, understand, and mitigate risks. We are intelligence analysts, incident responders, computer forensics experts, malware reverse engineers, journalists, linguists, academics, anti-fraud specialists, private investigators, lawyers, and former law-enforcement professionals. Through a full suite of products and services designed to protect organizations from sophisticated and everyday cyber threats, we integrate seamlessly into any client CTI program offering differing levels of integration from reports and data, collaborative force multiplication via managed service, or a fully outsourced CTI shop.

We solve the most difficult management and technology problems through a combination of consulting, analytics, digital solutions, engineering, and cyber expertise. With global headquarters in McLean, Virginia, our firm employs more than 23,300 people and had revenue of $5.80 billion for the 12 months ended March 31, 2017. To learn more, visit BoozAllen.com. (NYSE: BAH)