Forging the ShadowHammer

blog.reversinglabs.com/blog/forging-the-shadowhammer

Threat Research | March 27, 2019

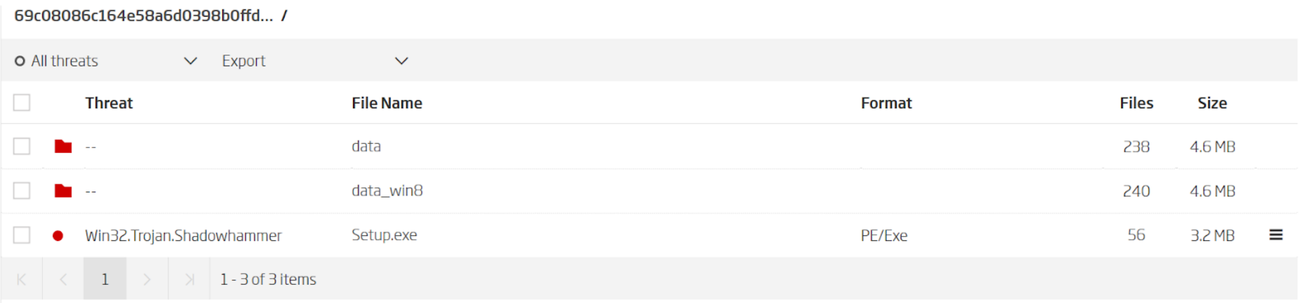
Blog Author

Tomislav Peričin, Chief Software Architect & Co-Founder at ReversingLabs. Read More...

Operation ShadowHammer is a new and highly targeted supply chain attack discovered by Kaspersky Lab. The attack leveraged ASUS Live Update software to distribute malicious code. Live Update is a utility which commonly comes pre-installed on most ASUS computers and is used to update system drivers and BIOS/UEFI code.

As the details of this supply chain attack are still unfolding our ReversingLabs researchers looked into what is currently publicly available. Using our Titanium Platform we've been able to make a few connections which lead us to, what we believe is, the first iteration of this malware code.

We started from the infected installation package that was published by Kaspersky Lab. Its content is the main installation file called Setup.exe and two additional MSI installation packages that contain all the software components that get installed on the system.

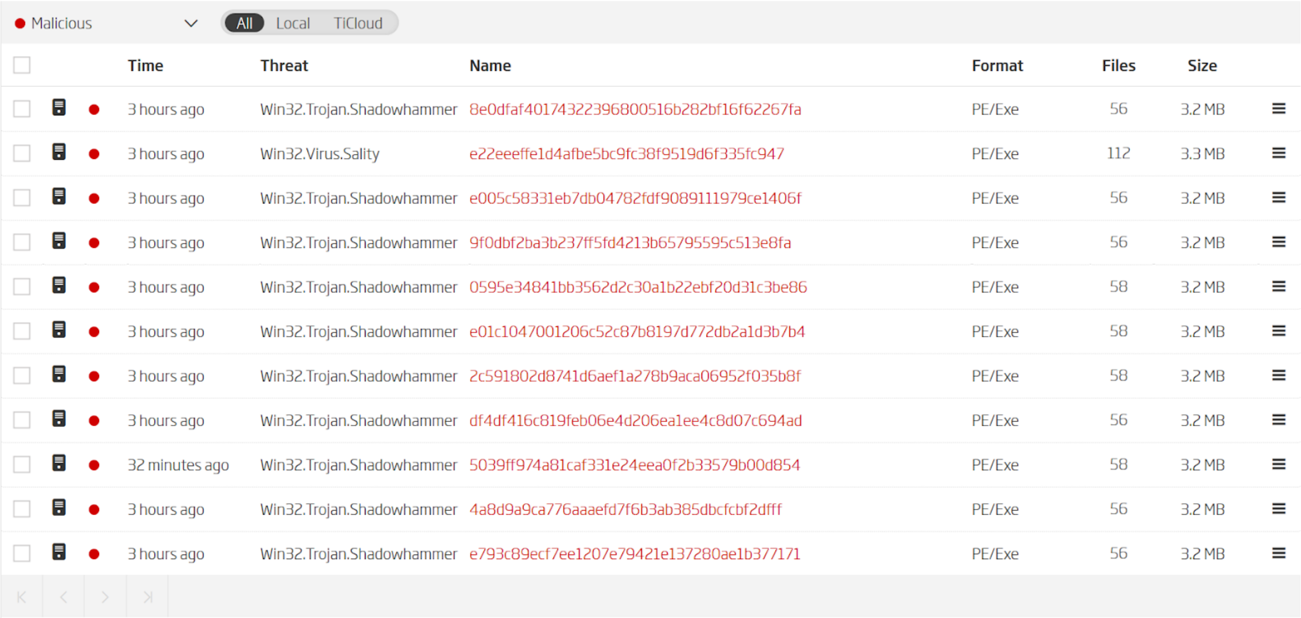

69c08086c164e58a6d0398b0ffd... /

□		Threat	File Name	Format	Files	Size	
□	📁	--	data		238	4.6 MB	
□	📁	--	data_win8		240	4.6 MB	
□	●	Win32.Trojan.Shadowhammer	Setup.exe	PE/Exe	56	3.2 MB	≡

1 - 3 of 3 items

Infected ASUS installation package - courtesy of Kaspersky Labs

The main executable file, Setup.exe, carries the malicious payload. Because of this, we decided to take a look at how we could pivot around Setup.exe and find additional samples to analyze. Using our RHA1 functional similarity algorithm we've been able to do just that and find 10 additional samples worth taking a closer look at.

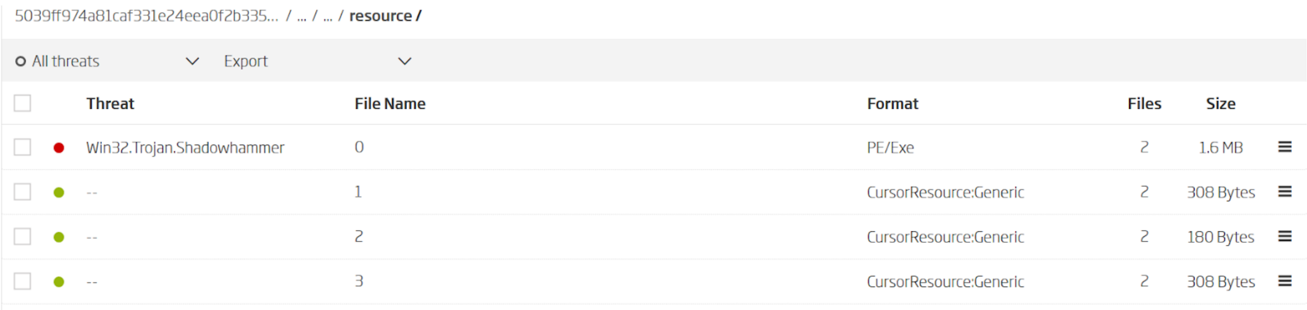


● Malicious ⌄ All Local TiCloud

□			Time	Threat	Name	Format	Files	Size	
□		●	3 hours ago	Win32.Trojan.Shadowhammer	8e0dfaf40174322396800516b282bf16f62267fa	PE/Exe	56	3.2 MB	≡
□		●	3 hours ago	Win32.Virus.Sality	e22eeeffe1d4afbe5bc9fc38f9519d6f335fc947	PE/Exe	112	3.3 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	e005c58331eb7db04782fdf9089111979ce1406f	PE/Exe	56	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	9f0dbf2ba3b237ff5fd4213b65795595c513e8fa	PE/Exe	56	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	0595e34841bb3562d2c30a1b22ebf20d31c3be86	PE/Exe	58	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	e01c1047001206c52c87b8197d772db2a1d3b7b4	PE/Exe	58	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	2c591802d8741d6aef1a278b9aca06952f035b8f	PE/Exe	58	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	df4df416c819feb06e4d206ea1ee4c8d07c694ad	PE/Exe	56	3.2 MB	≡
□		●	32 minutes ago	Win32.Trojan.Shadowhammer	5039ff974a81caf331e24eea0f2b33579b00d854	PE/Exe	58	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	4a8d9a9ca776aaaefd7f6b3ab385dbcfcbf2dfff	PE/Exe	56	3.2 MB	≡
□		●	3 hours ago	Win32.Trojan.Shadowhammer	e793c89ecf7ee1207e79421e137280ae1b377171	PE/Exe	56	3.2 MB	≡

Pivoting to find similar files via ReversingLabs RHA1 functional similarity algorithm

From this point, the investigation is carried forward by TitaniumCore, our advanced file decomposition engine. TitaniumCore has been able to extract embedded resources from all of the RHA1 detected installation packages. The installation packages which have 58 extracted files are particularly interesting as they contain one variant of the ShadowHammer attack.



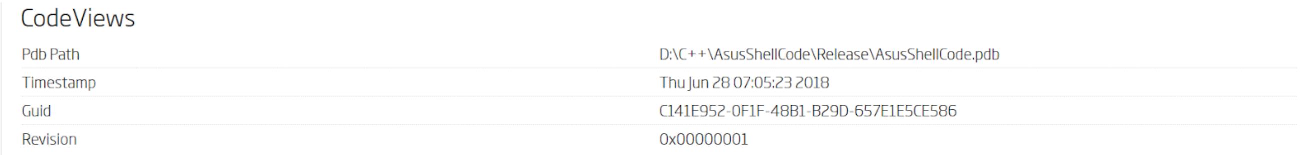
5039ff974a81caf331e24eea0f2b335... / ... / ... / resource /

○ All threats ⌄ Export ⌄

□		Threat	File Name	Format	Files	Size	
□	●	Win32.Trojan.Shadowhammer	0	PE/Exe	2	1.6 MB	≡
□	●	--	1	CursorResource:Generic	2	308 Bytes	≡
□	●	--	2	CursorResource:Generic	2	180 Bytes	≡
□	●	--	3	CursorResource:Generic	2	308 Bytes	≡

Extracted resources via ReversingLabs TitaniumCore static unpacking engine

This extracted executable is a Visual Studio C++ application that has been compiled with debug symbol information enabled. These symbols unveil a bit more about the attacker and the attack timeline.

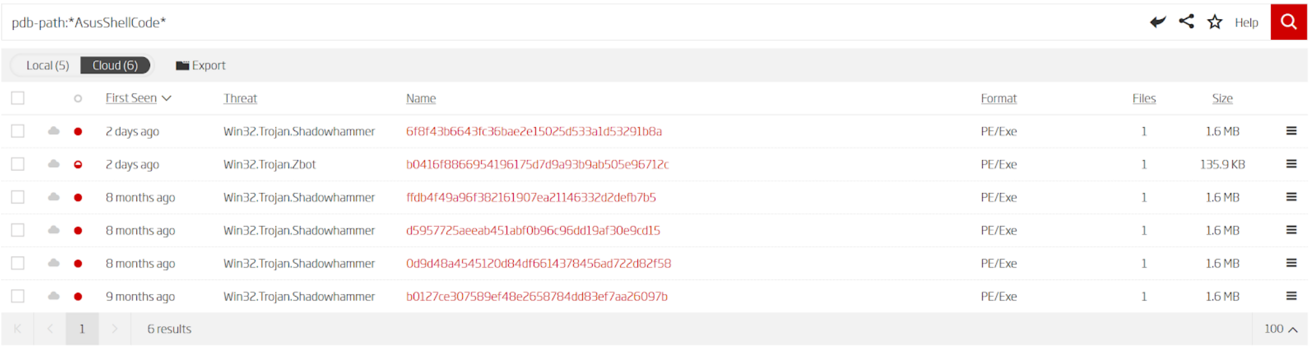


CodeViews

Pdb Path	D:\C++\AsusShellCode\Release\AsusShellCode.pdb
Timestamp	Thu Jun 28 07:05:23 2018
Guid	C141E952-0F1F-48B1-B29D-657E1E5CE586
Revision	0x00000001

PDB debugging information found within the extracted executable file

Based on the specifics of the file path, we were able to conclude that this is the original code the adversaries developed specifically to carry out this attack. Since PDB paths are indexed by our advanced search capabilities, finding all the other samples that share this path, requires only a simple one keyword search.

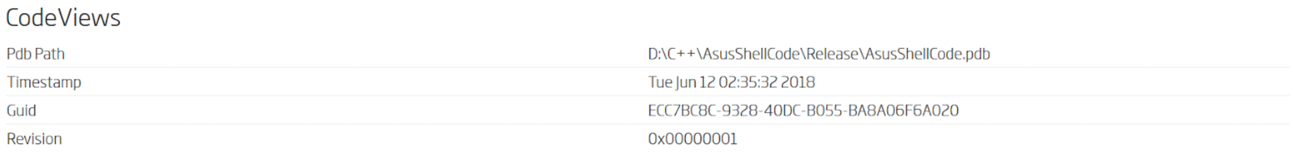


pdb-path:*AsusShellCode*

□		○	First Seen	Threat	Name	Format	Files	Size	
□		●	2 days ago	Win32.Trojan.Shadowhammer	6f8f43b6643fc36bae2e15025d533a1d53291b8a	PE/Exe	1	1.6 MB	≡
□		●	2 days ago	Win32.Trojan.Zbot	b0416f8866954196175d7d9a93b9ab505e96712c	PE/Exe	1	135.9 KB	≡
□		●	8 months ago	Win32.Trojan.Shadowhammer	ffdb4f49a96f382161907ea21146332d2defb7b5	PE/Exe	1	1.6 MB	≡
□		●	8 months ago	Win32.Trojan.Shadowhammer	d5957725aeeab451abf0b96c96dd19af30e9cd15	PE/Exe	1	1.6 MB	≡
□		●	8 months ago	Win32.Trojan.Shadowhammer	0d9d48a4545120d84df6614378456ad722d82f58	PE/Exe	1	1.6 MB	≡
□		●	9 months ago	Win32.Trojan.Shadowhammer	b0127ce307589ef48e2658784dd83ef7aa26097b	PE/Exe	1	1.6 MB	≡

Pivoting to other versions of the same malware via ReversingLabs Advanced Search

Within this batch of samples, we looked at the oldest one, which has the following debugging information.



CodeViews

Pdb Path	D:\C++\AsusShellCode\Release\AsusShellCode.pdb
Timestamp	Tue Jun 12 02:35:32 2018
Guid	ECC7BC8C-9328-40DC-B055-BA8A06F6A020
Revision	0x00000001

PDB debugging information found within the extracted executable file

The timestamp information within aligns perfectly with the attack timeline described by Kaspersky Lab.

The details of the attack are still being investigated by our own team and the teams of security researchers around the world. Our hope is that this short threat hunting blog will help those looking for more details as they put the pieces of this puzzle back together.

IOCs:

1bb53937fa4cba70f61dc53f85e4e25551bc811bf9821fc47d25de1be9fd286a
682fc8ccfc9316c54f02ae7865eee553ad0211031d4d80bb9c4365fbbc74049a
9acd43af36f2d38077258cb2ace42d6737b43be499367e90037f4605318325f8
6edc5578d824f42a6dd34664284179060f5595310fcb437a184f1ac0fc4fb1b4
cfbec77180bd67cceb2e17e64f8a8beec5e8875f47c41936b67a60093e07fcfd
c299b6dd210ab5779f3abd9d10544f9cae31cd5c6afc92c0fc16c8f43def7596

MORE BLOG ARTICLES