A Peek into BRONZE UNION's Toolbox

secureworks.com/research/a-peek-into-bronze-unions-toolbox

Threat Analysis
Wednesday, February 27, 2019 *By: Counter Threat Unit Research Team*

Summary

Secureworks® Counter Threat Unit™ (CTU) researchers have tracked the activities of the BRONZE UNION threat group (also known as Emissary Panda, APT 27, and LuckyMouse) since 2013. CTU™ analysis suggests that BRONZE UNION is located in the People's Republic of China. The threat group has historically leveraged a variety of publicly available and self-developed tools to gain access to targeted networks in pursuit of its political and military intelligence-collection objectives.

Breathing new life into old tools

In 2018, CTU researchers identified evidence of BRONZE UNION leveraging tools that have been publicly available for years. However, the variants used in 2018 included updated code.

ZxShell games

In mid-2018, CTU researchers observed BRONZE UNION deploying an updated version of the ZxShell remote access trojan (RAT). ZxShell was developed in 2006 by the persona "LZX", who then publicly released the source code in 2007. Although various threat actors have created different variations of the RAT, the version used by BRONZE UNION in 2018 contained some previously unobserved properties that suggest the threat group's capabilities continue to evolve:

- The malware embedded the well-known HTran packet redirection tool.
- The malware was signed with digital certificates that were signed by Hangzhou Shunwang Technology Co., Ltd (Serial: 29 f7 33 6f 60 92 3a f0 3e 31 f2 a5) and Shanghai Hintsoft Co., Ltd. (Serial: 09 89 c9 78 04 c9 3e c0 00 4e 28 43). These certificates are not exclusively used by BRONZE UNION but may indicate BRONZE UNION activity.

Figure 1 shows a session captured by Red Cloak™ where a BRONZE UNION threat actor launched a remote shell using ZxShell.

Figure 1. BRONZE UNION threat actor session. (Source: Secureworks)

"You look like you've seen a Gh0st RAT"

Like ZxShell, publicly available Gh0st RAT source code led to the emergence of several different variants. In a 2018 campaign, BRONZE UNION likely deployed modified Gh0st RAT malware to multiple systems within a compromised environment that were important to the threat actors' objective. When executed with administrator privileges, the Gh0st

RAT binary file was written to %System%\FastUserSwitchingCompatibilitysex.dll. The installer then created a Windows service and associated service dynamic link library (DLL) chosen from the names listed in Table 1.

Service name	DLL installed in %System%
Ias	Iassex.dll
Irmon	Irmonsex.dll
Nla	Nlasex.dll
Ntmssvc	Ntmssvcsex.dll
NWCWorkstation	NWCWorkstationsex.dll
Nwsapagent	Nwsapagentsex.dll
SRService	SRServicesex.dll
Wmi	Wmisex.dll
WmdmPmSp	WmdmPmSpsex.dll
LogonHours	LogonHourssex.dll
PCAudit	PCAuditsex.dll
helpsvc	helpsvcsex.dll
uploadmgr	uploadmgrsex.dll

Table 1. Service names and DLLs used by Gh0st RAT.

This Gh0st RAT sample communicated with IP address 43 . 242 . 35 . 16 on TCP port 443, although the traffic is a custom binary protocol and not HTTPS. The malware author also modified the standard Gh0st RAT headers to obfuscate the network traffic (see Figure 2).

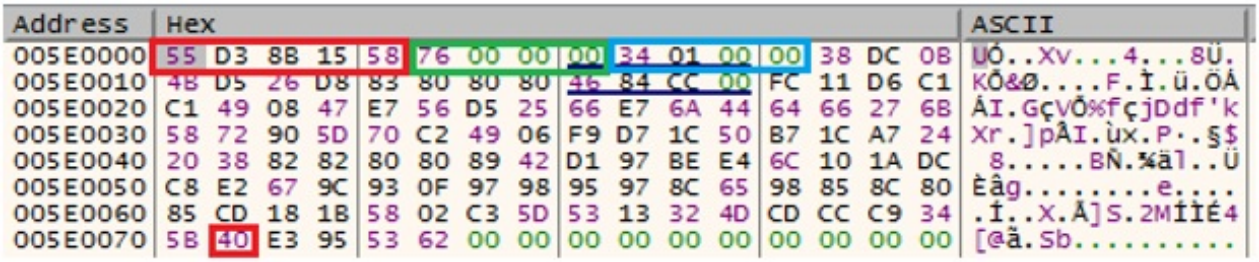

Figure 2. Gh0st RAT network traffic. (Source: Secureworks)

Bytes 0-4, which are typically known as the Gh0st RAT "identifier," are randomized in this case. Bytes 5-8 indicate the packet size, and bytes 9-12 indicate the zlib-decompressed packet size. In a departure from previous Gh0st RAT versions, the five bytes at the end of this packet are an XOR key, which must be applied to the packet data before the zlib decompression can be performed. The XOR key is different for each execution of the malware. Once the packet is decoded and decompressed, the data shown in Figure 3 is visible.

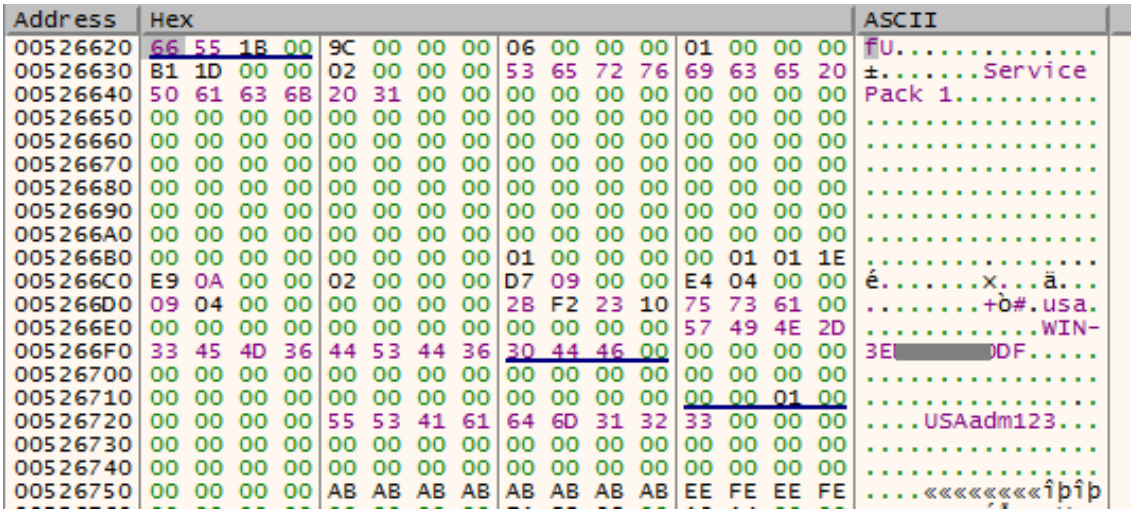

Figure 3. Decoded Gh0st RAT check-in packet. (Source: Secureworks)

The first byte of Figure 3 shows the value 0x66, which is the Gh0st RAT code for "login". After sending the initial phone-home request, Gh0st RAT exchanges 22-byte 'command' packets with its command and control (C2) server. Once again, the first five bytes are randomized and the zlib-compressed part of the packet is XOR-encoded, but the same identifiable structure remains. In the example command packet shown in Figure 4, the first five bytes are the randomized header and the next eight bytes show the compressed and uncompressed size of the data. The XOR key for this packet is 0x7c.

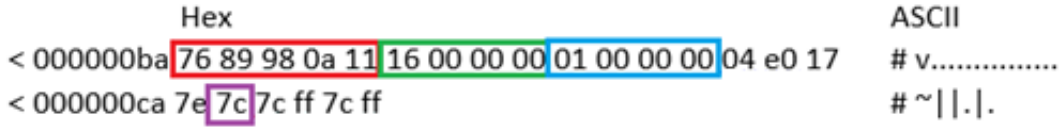

Figure 4. Gh0st RAT command packet. (Source: Secureworks)

Creating custom solutions

In addition to publicly available tools, BRONZE UNION has also used proprietary remote access tools such as SysUpdate and HyperBro since 2016. Despite self-developed tools generally benefitting from lower detection rates than publicly available tools, the threat actors appear to use their own tools more sparingly after securing consistent network access.

SysUpdate is a multi-stage malware used exclusively by BRONZE UNION. It has been delivered by multiple methods. In one instance observed by CTU researchers, it was downloaded by a malicious Word document using the Dynamic Data Exchange (DDE) embedded command method. In another incident, the threat actor manually deployed SysUpdate via previously stolen credentials after gaining access to the environment. In a third case, it was delivered via a redirect from a strategic web compromise (SWC). Regardless of the delivery method, the payload is a WinRAR self-extracting (SFX) file that installs the SysUpdate stage 1 payload.

The stage 1 payload is responsible for the following tasks:

- installing the stage 1 malware through DLL search-order hijacking
- setting up persistence by configuring either a registry Run key (see Figure 5) or an "Own Process" Windows service depending on privileges available at the time of installation
- contacting a C2 server to retrieve and install a second malware payload

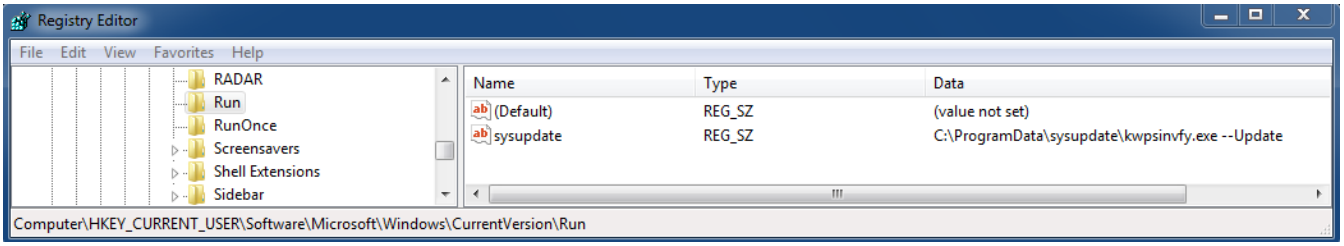

Figure 5. SysUpdate user-level Run key. (Source: Secureworks)

SysUpdate stage 1 has no capability beyond downloading the second payload file, SysUpdate Main (see Figure 6).

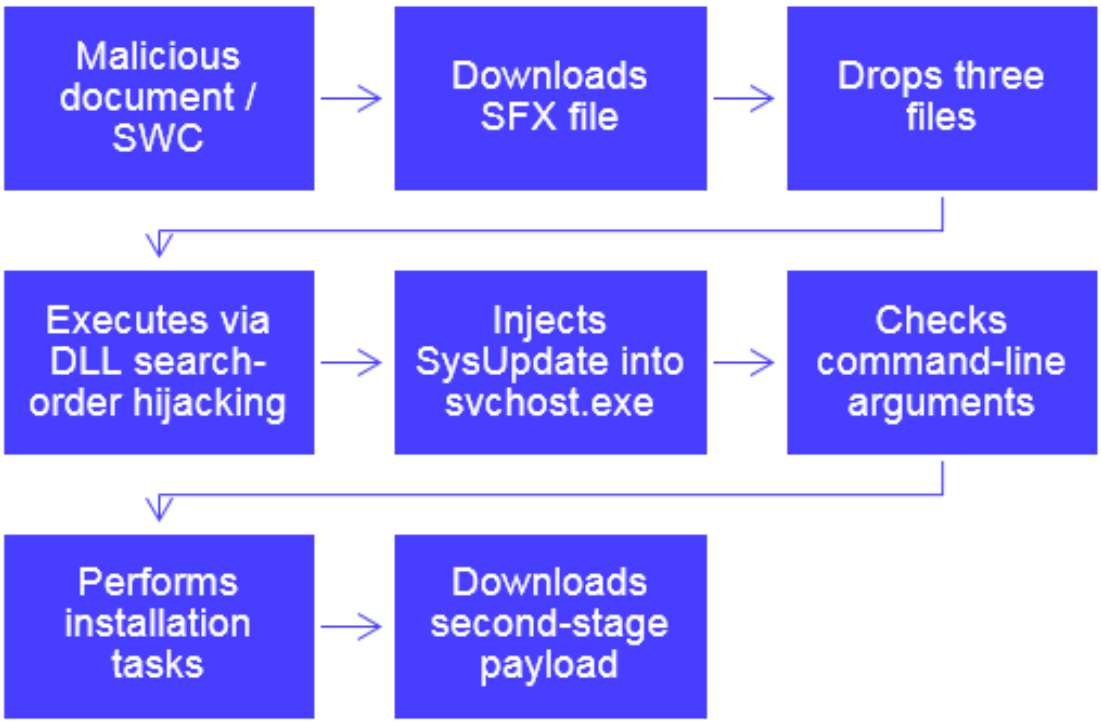

Figure 6. SysUpdate stage 1 installation process. (Source: Secureworks)

SysUpdate Main employs HTTP communications and uses the hard-coded User-Agent "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36". It downloads a file named m.bin using the HTTP GET method and injects this file into a new svchost.exe process without saving the file to disk. After performing this download, SysUpdate Main reverts to its binary protocol for any additional commands from the C2 server, beaconing every three minutes. The SysUpdate Main file analyzed by CTU researchers included remote access capabilities such as managing files and processes, launching a command shell, interacting with services, taking screenshots, and uploading and downloading additional malware payloads.

SysUpdate is flexible malware, as capabilities can be easily introduced and withdrawn by supplying a new payload file. The operator could remove second-stage capabilities at any time and revert to the first stage by supplying a replacement payload file. By withdrawing second-stage payloads when not in use, operators can limit exposure of their full capabilities if the malicious activity is detected.

Conclusion

BRONZE UNION was one of the most prolific and active targeted threat groups tracked by CTU researchers in 2017 and 2018. The threat actors have access to a wide range of tools, so they can operate flexibly and select tools appropriate for intrusion challenges. During complex intrusion scenarios, the threat actors leverage their proprietary tools, which offer custom functionality and lower detection rates. They appear to prefer using widely available tools and web shells to maintain access to networks over longer periods. After accessing a network, the threat actors are adept at circumventing common security controls, escalating privileges, and maintaining their access to high-value systems over long periods of time.

Threat indicators

The threat indicators in Table 2 are associated with BRONZE UNION activity. Note that IP addresses can be reallocated. The IP addresses and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
b7f958f93e2f297e717cffc2fe43f2e9	MD5 hash	ZxShell installer
fa53f09cd22b46b554762dc1a12c99dd692ec681	SHA1 hash	ZxShell installer
ef049339f1eb091cda335b51939f91e784e1ab1e006056d5a6bb526743b6cbc7	SHA256 hash	ZxShell installer
62bcbfae5276064615d0d45b895fdff2	MD5 hash	ZxShell service DLL (AudioSdk.dll)
9020e5010a916c6187597e9932402ed29098371c	SHA1 hash	ZxShell service DLL (AudioSdk.dll)
c2229a463637433451a3a50ccf3c888da8202058f5022ffd2b00fc411b395b79	SHA256 hash	ZxShell service DLL (AudioSdk.dll)
ae9c39e0d9a0c0ae48a72cb10521d2f3	MD5 hash	Malicious driver associated with ZxShell (autochk.sys)
2e80926d67ea68acb1df441be5ee1f2d86e7f92b	SHA1 hash	Malicious driver associated with ZxShell (autochk.sys)
b28c024db80cf3e7d5b24ccc9342014de19be990efe154ba9a7d17d9e158eecb	SHA256 hash	Malicious driver associated with ZxShell (autochk.sys)
language.wikaba.com	Domain name	ZxShell C2 server
solution.instanthq.com	Domain name	ZxShell C2 server
40cdd3cfe86c93872b163fb3550f47f6	MD5 hash	Gh0st RAT installer (T.exe)
ad2b27ea2fde31b1cc5104c01a21b22fef507c3d	SHA1 hash	Gh0st RAT installer (T.exe)
9a1437edd0493ff615a77b9ee1717c5f49ab0b28d1778898f591fb803655fbc6	SHA256 hash	Gh0st RAT installer (T.exe)
9c42cd7efbdfc47303d051f056c52d29	MD5 hash	Gh0st RAT binary (install.dll, FastUserSwitchingCompatibilitysex.dll)

Indicator	Type	Context
b8aa43dc92bec864c94442e6bf8c629c3bd0fe92	SHA1 hash	Gh0st RAT binary (install.dll, FastUserSwitchingCompatibilitysex.dll)
0b1217bd95678ca4e6f81952226a0cfd639ce4b2f7e7fce94ab177d42c5abf62	SHA256 hash	Gh0st RAT binary (install.dll, FastUserSwitchingCompatibilitysex.dll)
06348bbe0cc839f23c2d9471cfb19de3	MD5 hash	Gh0st RAT installer (Update.exe)
cd7c92ac0b36a8befa1b151537fc3fcdafca8606	SHA1 hash	Gh0st RAT installer (Update.exe)
b43ccd5b23d348f72466612d597ad71246113a9d524c9b27e682d1f7300a0672	SHA256 hash	Gh0st RAT installer (Update.exe)
43.242.35.16	IP address	Gh0st RAT C2 server observed in April 2018
103.85.27.78	IP address	Gh0st RAT C2 server observed in April 2018
trprivates.com	Domain name	SysUpdate C2 server sinkholed by CTU researchers
mildupdate.com	Domain name	SysUpdate C2 server sinkholed by CTU researchers
43.242.35.13	IP address	SysUpdate C2 server observed in late 2017
c8d83840b96f5a186e7bb6320e998f72	MD5 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
42e3fbff6f5576a3f4e8f941ea3dc00462d7838c	SHA1 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
938f32822c1a6b1140ac0af60a06ae39011464de37c511921d8a7d9c6a69c9df	SHA256 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
ef41da16fdedcc450d0cc6ca708a9222	MD5 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
714215d63b2f2d8f2caf94902af2f25452c21264	SHA1 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
0777fa4832ecf164029e23d0125b4fdc87e2f46ffc4e1badd6a45cf5be721660	SHA256 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
c25e8e4a2d5314ea55afd09845b3e886	MD5 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
e8cf3522b68a51b2aabcfc6f98b39da15a23da1d	SHA1 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION

Indicator	Type	Context
76bc063f8f348a202f92faac0c36f1a0a122f9b3568342abcd97651be7adec08	SHA256 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
88a27758f3066dd4da18983a005ddc20	MD5 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
1f9c979cbab9ff2519aa3bf3006a752177f4d8c6	SHA1 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
24a7e226f14fb86275b423d63d0332bfb95e261532f0667517c01da9d2bc51b3	SHA256 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
17acc1d983dde32b5bcde9c9624848b0	MD5 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
a03b14cac23dcfa2b2e12d5a8e53959d5a2e8fa2	SHA1 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
3f69c0e7392bc6441a308281b07627797613d89666a5c9b22cb104edf359c46b	SHA256 hash	SysUpdate installer (self-extracting RAR file) associated with BRONZE UNION
a13772805b772f374f7d709999a816d5	MD5 hash	Malicious SysUpdate DLL (Wsock32.dll) associated with BRONZE UNION
fa9600f1d15e61d5f2bdb8ac0399b7f42da63a01	SHA1 hash	Malicious SysUpdate DLL (Wsock32.dll) associated with BRONZE UNION
d40903560072bb777290d75d7e31a927f05924bffe00d26713c6b39e8e68ae82	SHA256 hash	Malicious SysUpdate DLL (Wsock32.dll) associated with BRONZE UNION
78142cdad08524475f710e5702827a66	MD5 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION
bc20da9465a7a7f9c2d5666ea5370c6c1e988441	SHA1 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION
3cebc9161e3e964a2e7651566c5a710d0625192ddecd14cfc5a873e7bc6db96f	SHA256 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION
0955e01bc26455965b682247ecb86add	MD5 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
23533c452b12131253e4e21f00ae082eba7cfdb3	SHA1 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
9d9c9c17ae4100b817a311ea0c6402e9f3eedc94741423796df3ead1375aaebf	SHA256 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
d4bb5c6364c4b4a07e6bbf2177129655	MD5 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION

Indicator	Type	Context
0689e40696a0cbecc5c3391e8b8b40d27a033186	SHA1 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION
dcfc9e4077705385328133557629fffee11662b7843b34dd4e1e42404ac2e921	SHA256 hash	Encrypted SysUpdate payload (sys.bin.url) associated with BRONZE UNION
cbb84d382724dd8adc5725dfca9b4af1	MD5 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
88de66897c448229b52c2ac991ba63e14fc3276b	SHA1 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
01926af0ff76607b3859734dda4b97fc55a8b8c2582982af786977929a414092	SHA256 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
8cb11e271aba3354545a77751c1e783e	MD5 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
e49833f2a4ec0422410a1c28ef58c9fc33c3a13f	SHA1 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
7f16b19f22ab0a33f9bf284aa0c2a9b9a429c4f4b7b801f2d2d80440eb74437f	SHA256 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
53d0db22c5abaf904d85facb70a60c8e	MD5 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
d363606e6159a786b06891227efac2164eeda7b3	SHA1 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
a941d46d6352fb2d70bba1423c4890dd5516e45d81f826900272ed14d0b678f4	SHA256 hash	Malicious SysUpdate DLL (pdh.dll) associated with BRONZE UNION
9814cdc7033a97fcf4f31aa377be60ba	MD5 hash	Malicious SysUpdate ActiveX control (LDVPOCX.OCX) associated with BRONZE UNION
2d568eb8ef17529e8bb6e658a032690e0f527d24	SHA1 hash	Malicious SysUpdate ActiveX control (LDVPOCX.OCX) associated with BRONZE UNION
9c1c798ba8b7f6f2334dcfcb8066be05d49c2e1395f7e7c8332e42afa708f5ae	SHA256 hash	Malicious SysUpdate ActiveX control (LDVPOCX.OCX) associated with BRONZE UNION
8b8e44bd5e4a9f7d58714ba9ca72351c	MD5 hash	Word document downloader (Final.docx) used by BRONZE UNION, associated with SysUpdate
02704ef94519eee0a57073b1e530ffea73df2a1f	SHA1 hash	Word document downloader (Final.docx) used by BRONZE UNION, associated with SysUpdate
86de90119b572620fd6a690b903c721679359cdc81f3d3327677e13539d5f626	SHA256 hash	Word document downloader (Final.docx) used by BRONZE UNION, associated with SysUpdate

Table 2. Indicators for this threat.