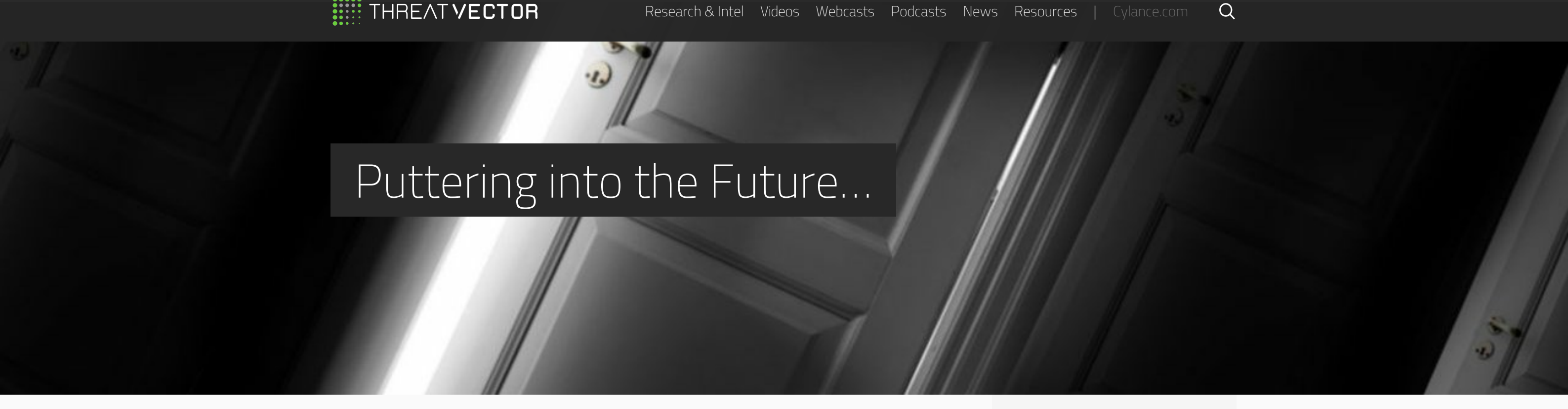


Puttering into the Future...

by Jon Gross and Jim Walter | January 12, 2016

Cyber-espionage has steadily migrated from a world of shadowy closed-door government players into the public spotlight over the past three years. Mandiant's APT1 report was the first to change the game, and paved the way for private security companies to expose advanced threat actors en masse. In the years since, both private security companies and media organizations alike have sought to capitalize on this craze. What is often neglected is reporting on the aftermath of such exposure, and what measures the attackers take to remain hidden, ready to strike again.

Very few reports offer follow-ups to what transpires after an attacker is completely pushed out of an environment. If they did, those reports would most likely paint a much bleaker picture of the cyberthreat landscape. The truth is most companies are never aware they've been breached again, even if they are hit multiple times after the initial attack. The truth is that intelligent attackers with long-term surveillance goals do not simply give up after their malware and command and control (C2) infrastructure is burned. Attackers typically redesign C2 infrastructure and deploy entirely new or updated malware after being exposed. Unless companies are well positioned to detect these changes, attackers will quietly slip back in time and time again.

At Cylance, we've become more interested in following the repercussions of public exposure of so-called advanced threat groups and malware, since this tends to be the new operational norm for security companies. While it's generally accepted that any exposure of coordinated cyber-espionage is a good thing, we believe it's not clear enough yet whether all the additional public attention is assisting or hindering cyber defenders. Intelligent attackers will adapt, modify tactics, and bolster their operational security in order to survive. We will err on the side of "it's generally better to know more than less", and will continue to explore the ramifications of public research to attacker activity over the months to come.

In 2014, our colleagues at Crowdstrike wrote an exposé about a long-standing Chinese APT threat group they self-named Putter Panda, which Mandiant/FireEye refers to as APT2. This threat group has been around for quite a while, and commonly operated tangentially to APT1 intrusions into defense contractors and aerospace companies. We've been tracking a series of exploit documents which, upon successful exploitation, simply drop a file and perform no other actions; these documents have dropped a variety of backdoors associated with a range of previously identified threat groups. One of them was of particular interest because we'd never seen the backdoor before and it leveraged a relatively unique German dynamic DNS provider for command and control.

The exploit document was targeted at a Russian speaker with the title "Гасий Константин Васильевич.doc", which roughly translates as "Gasy Konstantin", which seems to be someone's name. The document itself was a MIME-encoded HTML file which contained a base64-encoded word document as well as an appended XOR-encoded executable. The document exploited CVE-2012-0158 and will decode and write an executable to disk upon infection. The executable began at offset 0x9C50 in the MIME-document and used an encoding mechanism that consisted of an incrementing XOR key, starting at byte 0xAC combined with an additional XOR operation against the byte 0x28, which ultimately yields a unique 256-byte XOR key.

Document Details:

- Filename: Гасий Константин Васильевич.doc
- SHA256: 333061e6c4847aa72d3ba241c1df39aa41ce317a3d2898d3d13a5b6eccffc6d9
- File Size: 105,552 Bytes
- Author: User123

Upon successful exploitation, the backdoor is dropped to "%USERPROFILE%\Start Menu\Programs\Startup\time.exe". No other changes to the file system or registry are made. This method achieves persistence but the backdoor will not execute until the user logs off and back into the machine. This functionality alone can assist in the evasion of certain sandbox/dynamic analysis systems. Unless a live human can intervene in the sandboxing process, it would be impossible to observe the post-logoff behavior.

Backdoor Details:

- Filename: %USERPROFILE%\Start Menu\Programs\Startup\time.exe
- File Size: 40,960 Bytes
- SHA256: 523AD50B498BFB5AB688D9B1958C8058F905B634BEFC65E96F9F947E40893E5B
- Compile Time: 6/2/2015 7:21:08 UTC

Filename: Reappraisal_of_India_Tibet_Policy.doc
SHA256:
8d98155283c4d8373d2cf2c7b8a79302251a0ce76d227a8a2abdc2a244fc550e
File Size: 71680 bytes
Author: User
Filename: %temp%/kav.exe[2]
File Size: 18944 bytes
SHA256:
3d9bd26f5bd5401efa17690357f40054a3d7b438ce8c91367dbf469f0d9bd520
Compile Time: 3/7/2014 06:38:37 UTC
The above sample (kav.exe/wizard.exe) leverages **sys.firewall-gateway.net** for C2.

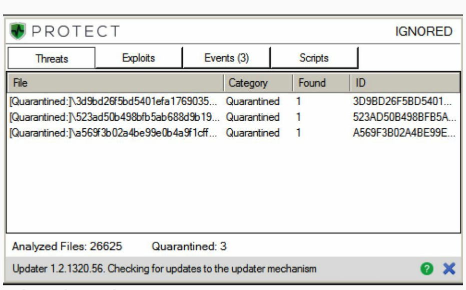
The German dynamic DNS provider supplies a number of free secondary domains for public use that network defenders should be on the lookout for, including:
*.firewall-gateway.com
*.firewall-gateway.de
*.firewall-gateway.net
*.kustomize.de
*.medical-dns.de
*.myfirewall.org
*.my-firewall.org
*.my-gateway.de
*.my-router.de
*.pptp.de
*.spdns.de
*.spdns.eu
*.spdns.org
*.spnoc.de
Current dynamic command and control infrastructure for these campaigns rely heavily upon the following domains and IP addresses:
Domains:
accounts-google.firewall-gateway.com
admin.spdns.org
creatnimei.dyndns-wiki.com
detail43.myfirewall.org
docs.google.com.publicvm.com
economy.spdns.de
economy.spdns.eu
extension.spdns.org
firefox.spdns.de
firewallupdate.firewall-gateway.net
intersecurity.firewall-gateway.com
jdk.spdns.eu
kaspersky.firewall-gateway.net
kissecurity.firewall-gateway.net
news.firewall-gateway.com
opero.spdns.org
sys.firewall-gateway.com
sys.firewall-gateway.net
tally.myfirewall.org
zuni.spdns.org
IP Addresses:
78.129.252.159
87.117.229.26
109.169.86.25

Conclusion

It's dangerous to develop a sense of "research malaise" when approaching piles of samples and the seemingly endless supply of malware we see and tear apart every day. Our many investigations have made us well aware that many regional threat actors employ, share, and recycle tools, techniques, and other identifiable bits of their tradecraft. Whether we refer to them as furry animals, numerals, or any other moniker, our investigations revealed a great deal of repetition. That being said, we know we must continue to be vigilant, considering the alarming fact that many of these known, familiar, and old techniques are still highly successful. Well-documented exploits from 2012 and 2013 are still working very effectively for these actors. Many of these antiquated exploits are still being used to deliver malware that is 100% undetected by the current AV industry, even though that industry continues to pat itself on the back for a job well done.

One of the goals of Cylance's SPEAR Team™ is to break down these "old" threats, reveal continued exposure to them, and demonstrate the value of thinking about countermeasures in a new way.

NOTE: These samples presented no problem for CylancePROTECT®:



File	Category	Found	ID
[Quarantined:]\3d9bd26f5bd5401efa1769035...	Quarantined	1	3D9BD26F5BD5401...
[Quarantined:]\523ad50b498bfb5ab688d9b19...	Quarantined	1	523AD50B498BFB5A...
[Quarantined:]\a569f3b02a4be99e0b4a9f1cff...	Quarantined	1	A569F3B02A4BE99E...

Analyzed Files: 26625 Quarantined: 3

Updater 1.2.1320.56. Checking for updates to the updater mechanism

Believe the math!!

[1] http://community.websense.com/blogs/securitylabs/archive/2013/08/15/tibetan-compromise.aspx

[2] Variations named "wizard.exe" are also commonly observed

The backdoor utilizes a few simple checks to ensure that Kaspersky products are not installed on the system, via a simple registry check looking for the key "HKLM\Software\KasperskyLab", as well as scanning running processes for a process named "avp.exe".

If both checks pass, the backdoor calls the API function SetTimer with a 10 second timeout. Once the timer elapses, a notification function is called. This notification function kills the timer and calls CreateThread with the start address of the backdoor code. The backdoor code is initially obfuscated by a single byte XOR against 0x61 where every even byte is skipped; control is then transferred to the second stage, which decrypts itself further using a single byte XOR with 0xB1. The backdoor will create an event named "Mi++(:v" and communicates to "aa123.spdns.de" on TCP port 8083.

At the time of this report, aa123.spdns.de resolved to "192.253.253.22". The backdoor appears to use its own custom binary protocol that begins with 128 bytes of data, which is further padded with 0x00's. Additional analysis into the protocol is ongoing.

A sample packet is presented below:

```
00000000  83 b2 68 0a 0a 19 3e 0b  d0 44 91 41 3d 3d a4 16 ..h...>. .D.A==..

00000010  89 b1 a0 96 32 73 02 ca  01 aa 84 a0 c2 37 35 1e ....2s.. .....75.

00000020  d6 3a 90 20 f0 1e e0 cf  4a 15 4b 2b 9b 68 67 25 .:. .... J.K+.hg%

00000030  87 35 f7 5e 86 fa 0b 05  8f 8e b2 c4 3a 9d 1e 88 .5.^.... ....:...

00000040  48 bf 4e 86 d8 1e 6b 1f  18 96 0f 60 3f 9e a1 d3 H.N...k. ...`?...

00000050  9d f4 80 9a b3 fd 6f 97  ce b0 f7 e9 ab a7 60 96 ......o. ......`.

00000060  81 68 47 ff a5 0b 68 b8  af 29 9b 46 54 dd 49 0c .hG...h. .).FT.I.

00000070  28 32 91 a2 21 b9 63 72  9b 94 d6 27 24 4c dc 91 (2..!.cr ...'$L..

00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........

---Truncated---
```

Also of interest is the fact that this and similar backdoors currently have zero detection by current antivirus vendors. This was verified recently a second time as we were reviewing the research in January 2016.

In addition, of particular note is the fact one Chinese AV firm briefly detected this sample when it was rescanned on July 14, 2015, and quickly corrected that detection by July 21st, behaving as if it were a false detection. As the investigation continued, we were able to identify more publically available backdoors of the same type.

Backdoor Details:

Filename: %USERPROFILE%\Start Menu\Programs\Startup\time.exe

File Size: 40,960 Bytes

SHA256:
A569F3B02A4BE99E0B4A9F1CFF43115DA803F0660DD4DF114B624316F3F63DC6

Compile Time: 5/18/2015 8:11:57 UTC

Although compiled earlier in time, this file (A569F3B02A4BE99E0B4A9F1CFF43115DA803F0660DD4DF114B624316F3F63DC6) is virtually identical from a functionality perspective. It used the byte 0x4D to XOR decode the second stage of malicious code and was configured to beacon to opero.spdns.org and firefox.spdns.de. Also of slight difference was the event it created, which was named "ZFhyBPk".

Ties to Tibet-Themed Watering Hole Campaign

Very similar behavior (in terms of the first few stages of attack) can be observed in previously analyzed attacks[1]which center on pro-Tibet and other Tibetan-related targets. The campaigns are also linked by C2 servers (largely *.firewall-gateway.com and *.myfirewall.org) and by the post-exploitation behavior of the installed tools.

Example:

Document Details:

Backdoor Details:

Share It:

Threat Research

About The Author

Jon Gross
Jon Gross is the Director of Threat Intelligence at Cylance.
Author's Bio

Jim Walter
Jim Walter is a Senior Security Researcher at Cylance.

Author's Bio

BlackBerry | CYLANCE
400 Spectrum Center Dr., Suite #900
Irvine, CA 92618
1-844-CYLANCE
1-844-295-2623

Blog
Home
News Bites
Videos
Resources
Cylance News
Webcasts
Podcasts
Contributors

Company
Who We Are
Resource Center
Cylance News
Press Releases
Privacy Notice
Terms of Service

Products
CylancePROTECT
CylanceOPTICS
Cylance ThreatZERO
Cylance Smart Antivirus

Services
Consulting Overview
Industry Overview