Researchers Discover New variants of APT34 Malware

boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html

Table 1. Relationship between original binary and three discovered variants. (Use the scrollbar to view the content on the far right.)

As you can see from Table 1 above, these files exhibit many similar characteristics and behaviors. Most of the differences appear to be cosmetic and do not affect the underlying functionality. Our analysts took a closer look at the C2 domain poison-frog[.]club, which is used in 3 of the 4 files, and found that it overlaps with the findings of the FireEye report. The domain resolved to 82.102.14.219 from at least August 2017 until December 2017. Additional domains that resolved to that IP during that time frame are dns-update[.]club, hpserver[.]online, and anyportals[.]com which were all mentioned in the FireEye report. The other C2 domain used, proxycheker[.]pro, resolved to 94.23.172.164 and 185.15.247.147, with 185.15.247.147 also hosting dns-update[.]club during that time frame. This new-found evidence, in combination with similar versions of POWRUNER and BONDUPDATER, the existence of the same debug strings in the code of each variant, and the overlapping infrastructure indicate that these three new binaries are also associated with APT34 operations.

The DGA domain generation algorithm used in one version of the BONDUPDATER backdoor is broken down into two parts: send and receive. If data is being sent, then the following format is used:

000C20009204A601	7D	A	56	7	6556666775466767667566765657661c79e4f73cd932f3f64ca161c45041	336662009e6a	.poison-frog.club
1	2	3	4	5	6	7	8

Use the scrollbar to view the content on the far right.

1. This is created from combining a unique ID (generated from the MAC address or encoded version of whoami) along with two other parameters which are inserted at two different random offsets in the unique ID
2. Random characters generated from: -join ((48 .. 57)+(65 .. 70) | Get-Random -Count (%{ Get-Random -InputObject (1 .. 7) }) | %{ [char]$_ })
3. Hardcoded "A"
4. Two random offset values referenced in #1.
5. Hardcoded "7"
6. Data Chunk being sent
7. Encoded Filename being sent
8. Hardcoded domain ".poison-frog[.]club"

If data is being received, then the following format is used:

1. This is created from combining a unique ID (generated from the MAC address or encoded version of whoami) along with two other parameters which are inserted at two different random offsets in the unique ID
2. Random characters generated from: -join ((48 .. 57)+(65 .. 70) | Get-Random -Count (%{ Get-Random -InputObject (1 .. 7) }) | %{ [char]$_ })
3. Hardcoded "A"
4. Two random offset values referenced in #1.
5. Hardcoded "7"
6. Hardcoded domain ".poison-frog[.]club"

The Domain Generating Algorithm (DGA) generation process is different than what was previously mentioned in the FireEye report. However, it would still be detected using DarkLabs' custom DGA detection mechanism.

In early January 2018, ClearSky Cyber Security tweeted about two new malware samples attributed to Oilrig/APT34. These samples were being deployed via a malicious .chm (Compiled HTML Help File) file. ClearSky provides a link to a Google document they use for "Raw Threat Intelligence" which contained additional IOCs associated with this campaign. Two hashes provided in that document are for versions of POWRUNER (MD5: BED81E58EF8FF0B073E371D433A08855) and BONDUPDATER (MD5: 63D6B1933F7330358A8FBFAF77532133). These two backdoors contain a reference to another C2 domain, www.window5[.]win. Using the custom tool developed in DarkLabs, we were able to pivot from these samples and discover an additional sample each of POWRUNER and BONDUPDATER.

These two new samples exhibit similar behavior to the samples mentioned in the FireEye report. However, there are a few slight differences - namely the use of a new C2 domain and URI, www.window5[.]win/update.aspx. At writing time of this post, that domain resolves to 185.181.8.246. Current research indicates that IP does not host any other domains publicly available. Additionally, the %PUBLIC%\Java location (e.g. C:\Users\Public\Java) is used for a staging directory in this version of POWRUNER.

IOC - Network

Domain/IP Address	Description
proxycheker[.]pro	C2
poison-frog[.]club	C2
window5[.]win	C2
82.102.14.219	Has resolved poison-frog[.]club, dns-update[.]club, hpserver[.]online & anyportals[.]com
94.23.172.164	Has resolved proxycheker[.]pro
185.15.247.147	Has resolved proxycheker[.]pro & dns-update[.]club
185.181.8.246	Has resolved window5[.]win

IOC - Endpoint

Filename	Description	MD5 Hash
dupdatechecker.exe	Dropper of POWRUNER and BONDUPDATER	C9F16F0BE8C77F0170B9B6CE876ED7FB
exeruner_new.exe	Dropper of POWRUNER and BONDUPDATER	87FB0C1E0DE46177390DE3EE18608B21
exeruner.exe	Dropper of POWRUNER and BONDUPDATER	A602A7B6DEADC3DFB6473A94D7EDC9E4
exeruner_new.exe	Dropper of POWRUNER	4EA656D10BE1D6EAC05D69252D270592
GoogleUpdateschecker.vbs	Deploys POWRUNER	6F2CA6D892CCA631C191233CB89D9B93
JavaUpdates	Scheduled Task to run VBS script	0681F2459EDF28DCD99493AE8A6398D5
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER	EE93A172937D37D3152D694331E59A21
GoogleUpdateTasks.vbs	Deploys POWRUNER and BONDUPDATER	F0B278427C8841C5D1A79ED2631B1522
JavaUpdatesTasksHosts	Scheduled Task to run VBS script	52973212E6373585F55B4DD207D890FF
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	06D537AF8C43F65FC467781B01047E5C
GoogleUpdateschecker.vbs	Deploys POWRUNER and BONDUPDATER	33E86AB6621F3DB7CD7E37CAF42C95E5
JavaUpdates	Scheduled Task to run VBS script	517D1D51414019272849E7C67E622597
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	614DDCCDCAF73172C1216D812595394C
UpdateCheckers.ps1	BONDUPDATER	1DE8F76404EB799C780DA5830915A17E
dUpdateCheckers.ps1	BONDUPDATER	27ACDFAB0A264B4EBD4DD16DAE6C4E0E
GoogleUpdates.vbs	Deploys POWRUNER and BONDUPDATER	D9BBB27B0C5249D681179D234BFF60DE
JavaUpdatesTask	Scheduled Task to run VBS script	347929555E8D7174D82356F47A054106
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	C3572009CA311F44A99C4FAB3F3DFF92
hxyz.ps1	POWRUNER	BED81E58EF8FF0B073E371D433A08855
dxyz.ps1	BONDUPDATER	63D6B1933F7330358A8FBFAF77532133
unknown	POWRUNER	CBE2F69D9EF39093D8645D3C93FD7F21
unknown	BONDUPDATER	277FF86501B98A4FF8C945AC4D4A7C53
Yara Signature for the dropper	{ strings: $exeruner_string_1 = "C:\\Users\\aaa\\documents\\visual studio 2015\\Projects\\exeruner\\exeruner\\obj\\Debug\\exeruner.pdb" $exeruner_string_2 = "C:\\Users\\aaa\\Desktop\\test\\exeruner\\exeruner\\obj\\Debug\\exeruner_new.pdb" condition: $exeruner_string_1 or $exeruner_string_2 }	

Source	Hash Value	C2 Domain	Details
FireEye Report	C9F16F0BE8C77F0170B9B6CE876ED7FB	proxychecker[.]pro	• Contains both POWRUNER and BONDUPDATER • Communicates with C2 via proxychecker[.]pro/update_wapp.aspx • POWRUNER appears to not have the ability to save files
ATH Tool	87FB0C1E0DE46177390DE3EE18608B21	poison-frog[.]club	• Contains both POWRUNER and BONDUPDATER • Communicates with C2 via poison-frog[.]club/update_wapp.aspx • POWRUNER appears to not have the ability to save files
ATH Tool	A602A7B6DEADC3DFB6473A94D7EDC9E4	poison-frog[.]club	• Contains both POWRUNER and BONDUPDATER • Communicates with C2 via poison-frog[.]club/update_wapp.aspx • POWRUNER appears to not have the ability to save files
RetroHunt	4EA656D10BEAC05D69252D270592	poison-frog[.]club	• Contains only POWRUNER • Communicates with C2 via poison-frog[.]club/update_wapp.aspx • POWRUNER appears to not have the ability to save files • POWRUNER contains more Base64 obfuscation effort than other versions

000C20009204A601	7D	A	56	7	6556666775466767667566765657661c79e4f73cd932f3f64ca161c45041			336662009e6a	.poison-frog.club
1	2	3	4	5	6			7	8

0800C0092904A601	02	A	51	7	.poison-frog.club
1	2	3	4	5	6

Source	Hash Value	C2 Domain	Details
ClearSky Cyber Security	BED81E58EF8FF0B073E371D433A08855	window5[.]win	• POWRUNER • Communicates with C2 via www.window5[.]win/update.aspx
ClearSky Cyber Security	63D6B1933F7330358A8FBFAF77532133	window5[.]win	• BOUNDATER • Communicates via DGA based DNS to wondow5[.]win
ATH Tool	CBE2F69D9EF39093D8645D3C93FD7F21	window5[.]win	• POWRUNER • Communicates with C2 via www.window5[.]win/update.aspx
ATH Tool	277FF86501B98A4FF8C945AC4D4A7C53	window5[.]win	• BONDUPDATER • Communicates via DGA based DNS to window5[.]win

Table 2. Relationship between original two samples and two discovered variants. (Use the scrollbar to view the content on the far right.)

IOC - Network

Domain/IP Address	Description
proxycheker[.]pro	C2
poison-frog[.]club	C2
window5[.]win	C2
82.102.14.219	Has resolved poison-frog[.]club, dns-update[.]club, hpserver[.]online & anyportals[.]com
94.23.172.164	Has resolved proxycheker[.]pro
185.15.247.147	Has resolved proxycheker[.]pro & dns-update[.]club
185.181.8.246	Has resolved window5[.]win

IOC - Endpoint

Filename	Description	MD5 Hash
dupdatechecker.exe	Dropper of POWRUNER and BONDUPDATER	C9F16F0BE8C77F0170B9B6
exeruner_new.exe	Dropper of POWRUNER and BONDUPDATER	87FB0C1E0DE46177390DE3
exeruner.exe	Dropper of POWRUNER and BONDUPDATER	A602A7B6DEADC3DFB6473
exeruner_new.exe	Dropper of POWRUNER	4EA656D10BE1D6EAC05D6
GoogleUpdateschecker.vbs	Deploys POWRUNER	6F2CA6D892CCA631C19123

JavaUpdates	Scheduled Task to run VBS script	0681F2459EDF28DCD99493
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER	EE93A172937D37D3152D69
GoogleUpdateTasks.vbs	Deploys POWRUNER and BONDUPDATER	F0B278427C8841C5D1A79E
JavaUpdatesTasksHosts	Scheduled Task to run VBS script	52973212E6373585F55B4DD
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	06D537AF8C43F65FC46778
GoogleUpdateschecker.vbs	Deploys POWRUNER and BONDUPDATER	33E86AB6621F3DB7CD7E37
JavaUpdates	Scheduled Task to run VBS script	517D1D51414019272849E7C
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	614DDCCDCAF73172C1216
UpdateCheckers.ps1	BONDUPDATER	1DE8F76404EB799C780DA5
dUpdateCheckers.ps1	BONDUPDATER	27ACDFAB0A264B4EBD4DD
GoogleUpdates.vbs	Deploys POWRUNER and BONDUPDATER	D9BBB27B0C5249D681179D
JavaUpdatesTask	Scheduled Task to run VBS script	347929555E8D7174D82356F
rUpdateChecker.ps1	Sets up scheduled task to deploy POWRUNER and BONDUPDATER	C3572009CA311F44A99C4F
hxyz.ps1	POWRUNER	BED81E58EF8FF0B073E371
dxyz.ps1	BONDUPDATER	63D6B1933F7330358A8FBF
unknown	POWRUNER	CBE2F69D9EF39093D8645D
unknown	BONDUPDATER	277FF86501B98A4FF8C945
Yara Signature for the dropper	{ strings: $exeruner_string_1 = "C:\\Users\\aaa\\documents\\visual studio 2015\\Projects\\exeruner\\exeruner\\obj\\Debug\\exeruner.pdb" $exeruner_string_2 = "C:\\Users\\aaa\\Desktop\\test\\exeruner\\exeruner\\obj\\Debug\\exeruner_new.pdb" condition: $exeruner_string_1 or $exeruner_string_2 }	

Use the scrollbar to view the content on the far right.

By diving deeper and pivoting on known indicators using techniques developed and honed by our experienced analysts, the indicator lifecycle can diversify discovery. In this case, analysts discovered additional unreported, yet campaign associated IOCs that can be used for further detection. Additionally, our analysts also developed YARA signatures for static detection, and TTP based signatures to deploy to EDR tools or for hunting through endpoint telemetry data.

The Booz Allen DarkLabs Threat Hunt team recommends deploying detection to endpoints for the hashes listed above and perform a retroactive search for the domains and IPs in SIEM logs. We also recommend the use of telemetry data collected via EDR tools to continuously hunt for this behavior. Monitoring for the behavior or TTP is a critical step because although IOCs can be used for detection and discovery, they can in many cases be changed cheaply and easily. Our advanced Threat Hunt team always recommends a robust proactive approach to threat hunting with a focus on behavioral detection.

Please contact us if you would like to learn more about DarkLabs Threat Hunt team or if you are interested in joining our team.

Expert in the Field

Garrettson Blight

Detecting A New Advanced Persistent Threat: Adware
Get tips on how to identify a new, sophisticated adware variant, and learn what to do if you find it in your network. Read More

What's It Take to Be a Cyber Elite?
Our ability to recruit and retain top-tier cyber talent allows us to build teams with the true diversity of skill sets required to overcome our clients' toughest, most specialized cybersecurity challenges. Read More