Catching lateral movement in internal emails

blog.reversinglabs.com/blog/catching-lateral-movement-in-internal-emails

Threat Research | August 5, 2019

Blog Author

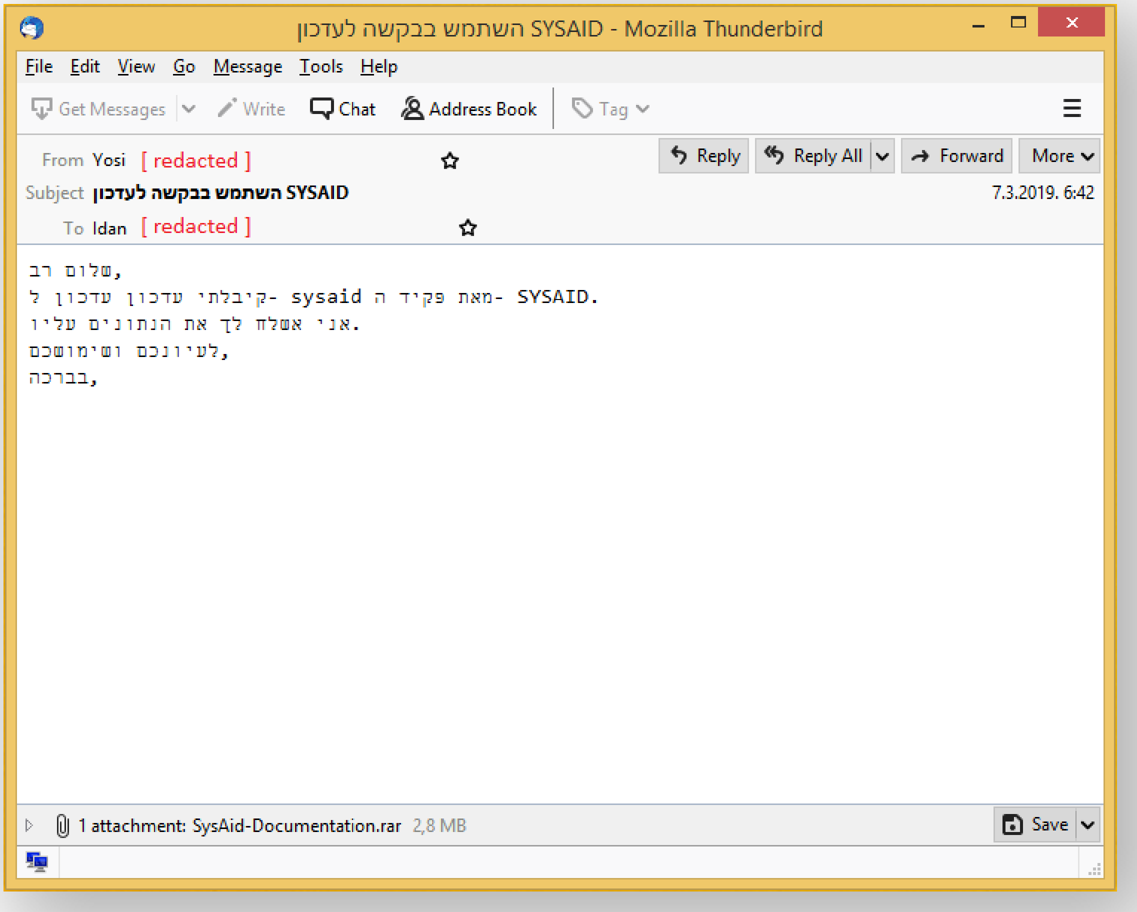
Tomislav Peričin, Chief Software Architect & Co-Founder at ReversingLabs. Read More...

Email-based attacks are the most prominent threat vector that organizations see today. Like any other form of communication, emails get exploited to become carriers for a wide variety of attacks. Securing email nowadays means worrying about malicious attachments, links leading to malware, links leading to phishing sites, and business email compromise attacks.

Due to their nature, those attacks are commonly perceived as threats external to the organization. However, when the organization is already compromised, internal emails can become a tool used by the attacker to move laterally through the organization. In some cases, they are the stealthiest choice, as some organizations only perform security checks against incoming emails.

The following analysis is a reconstruction of an attack on a manufacturing company with ties to aerospace and defense industries.

Yosi and Idan both work for a compromised manufacturing company. Yosi, a mechanical engineer, is sending an email to Idan. He is notifying his colleague about changes to their helpdesk software. The email contains a short message about the documentation that he’s attached.


השתמש בבקשה לעדכון SYSAID - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Save

From Yosi [redacted]

Subject השתמש בבקשה לעדכון SYSAID

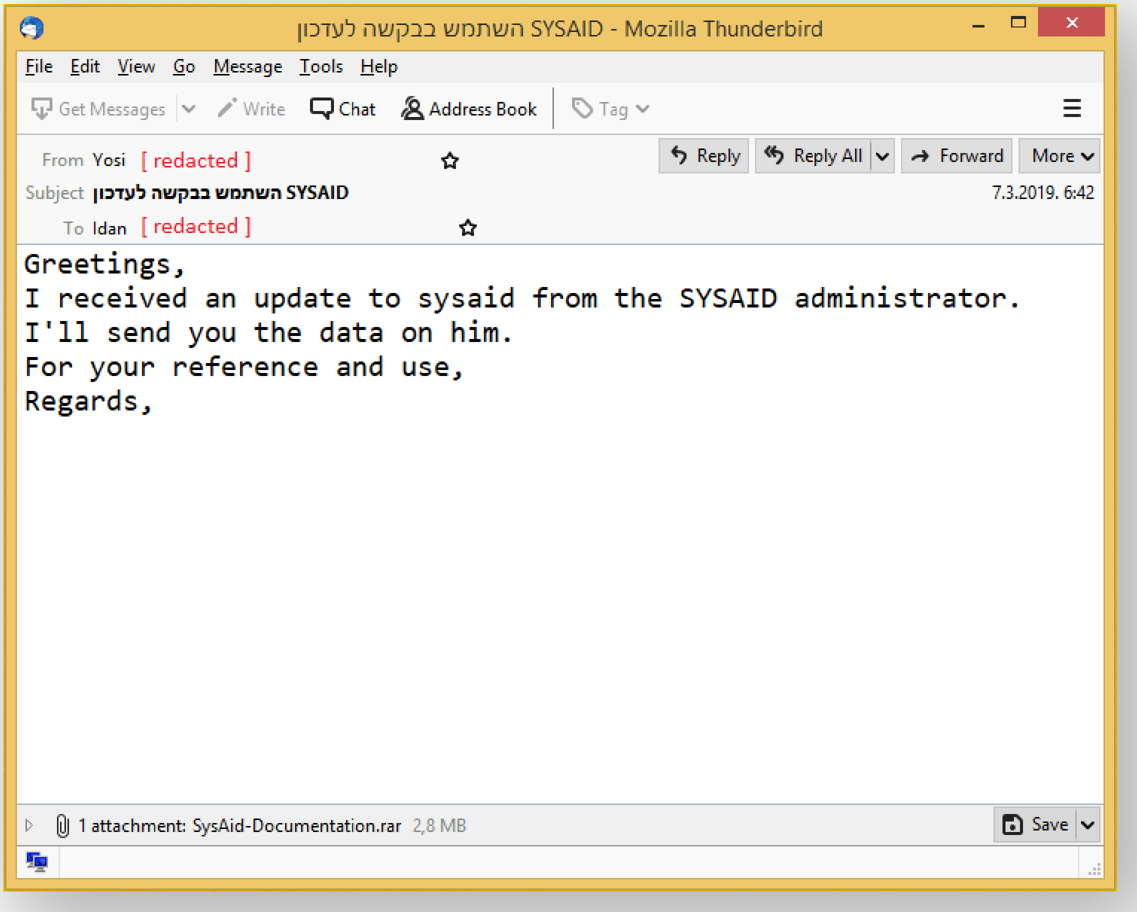
7.3.2019. 6:42

To Idan [redacted]

שלום רב,
קיבלתי עדכון עדכון ל- sysaid מאת פקיד ה- SYSAID.
אני אשלח לך את הנתונים עליו.
לעיונכם ושימושכם,
בברכה,

1 attachment: SysAid-Documentation.rar 2,8 MB

When run through an automated language translation service, the message reads something like this.


השתמש בבקשה לעדכון SYSAID - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Save

From Yosi [redacted]
Subject השתמש בבקשה לעדכון SYSAID
To Idan [redacted]
7.3.2019. 6:42

```
Greetings,
I received an update to sysaid from the SYSAID administrator.
I'll send you the data on him.
For your reference and use,
Regards,
```

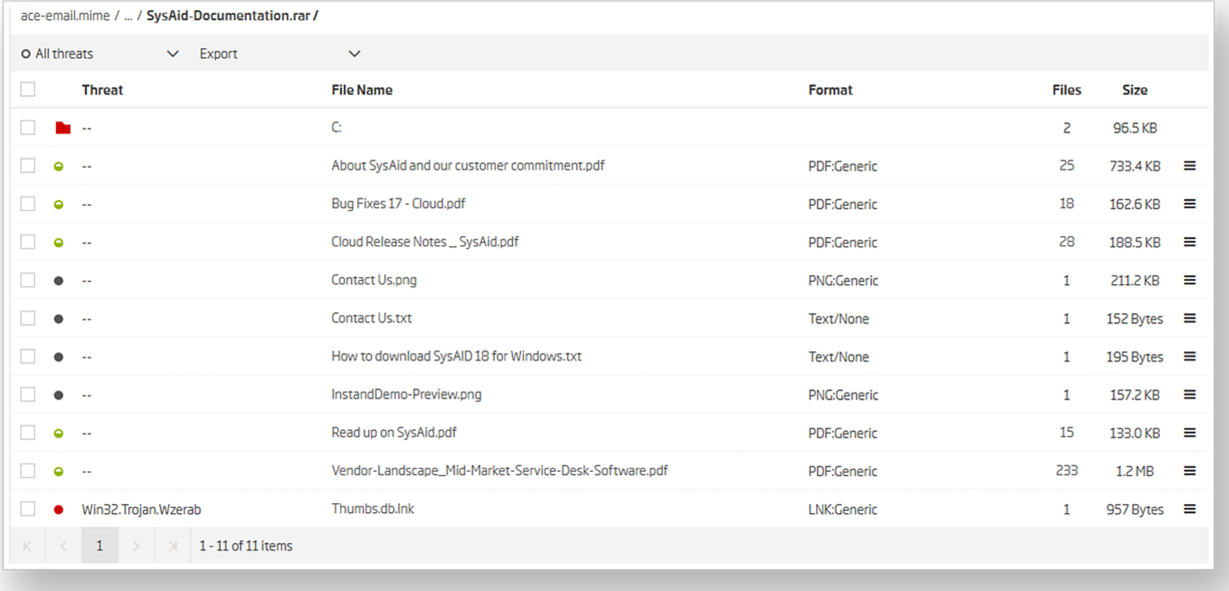
1 attachment: SysAid-Documentation.rar 2,8 MB

Sounds quite convincing. Since Idan trusts his coworker Yosi, he feels comfortable opening the attachment. There's no reason for Idan to suspect that Yosi isn't the one sending him the email. The email is sent from Yosi's email address; it has the same reply-to address. Even if Idan put in the extra effort to inspect the email headers, all he would see is that the email was routed through the internal mail server.

However, that attachment is not a RAR archive despite its file extension. In reality, it is an ACE archive - a format that WinRAR knows how to open. Within WinRAR, the ACE format support is provided by a freeware library made by the WinACE authors.

That library has recently been found to be affected by a path traversal vulnerability - an issue that allows an attacker to place a file in an arbitrary folder on the system. This vulnerability can be used to place an executable file in just the right place for it to launch the next time the machine powers up. That is exactly what the attachment is trying to do.

ReversingLabs A1000 visualizes the email headers and allows analysts to browse email contents. Email attachments - when they are an archive - are extracted and displayed in a view similar to one of an archive manager. The image below shows the contents of the ACE archive Yosi sent to Idan.



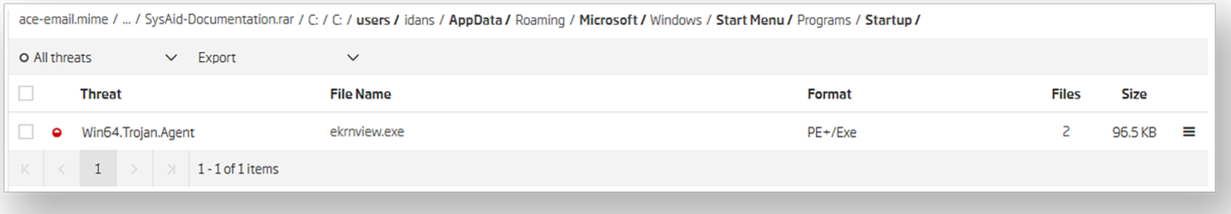
ace-email.mime / ... / SysAid-Documentation.rar /

	Threat	File Name	Format	Files	Size
▆	--	C:		2	96.5 KB
●	--	About SysAid and our customer commitment.pdf	PDF:Generic	25	733.4 KB
●	--	Bug Fixes 17 - Cloud.pdf	PDF:Generic	18	162.6 KB
●	--	Cloud Release Notes _ SysAid.pdf	PDF:Generic	28	188.5 KB
●	--	Contact Us.png	PNG:Generic	1	211.2 KB
●	--	Contact Us.txt	Text/None	1	152 Bytes
●	--	How to download SysAID 18 for Windows.txt	Text/None	1	195 Bytes
●	--	InstandDemo-Preview.png	PNG:Generic	1	157.2 KB
●	--	Read up on SysAid.pdf	PDF:Generic	15	133.0 KB
●	--	Vendor-Landscape_Mid-Market-Service-Desk-Software.pdf	PDF:Generic	233	1.2 MB
●	Win32.Trojan.Wzerab	Thumbs.db.lnk	LNK:Generic	1	957 Bytes

1 - 11 of 11 items

The documentation that Yosi promised to Idan is certainly there. There's lots of it, and it is used to cover the fact that Yosi is not who he claims to be. The first folder in the list of files is an indication that the attached ACE archive is exploiting the path traversal vulnerability - assigned CVE-2018-20250.

Following the folder path all the way down, it is easy to see where the following executable file is going to be extracted to.



ace-email.mime / ... / SysAid-Documentation.rar / C: / C: / users / idans / AppData / Roaming / Microsoft / Windows / Start Menu / Programs / Startup /

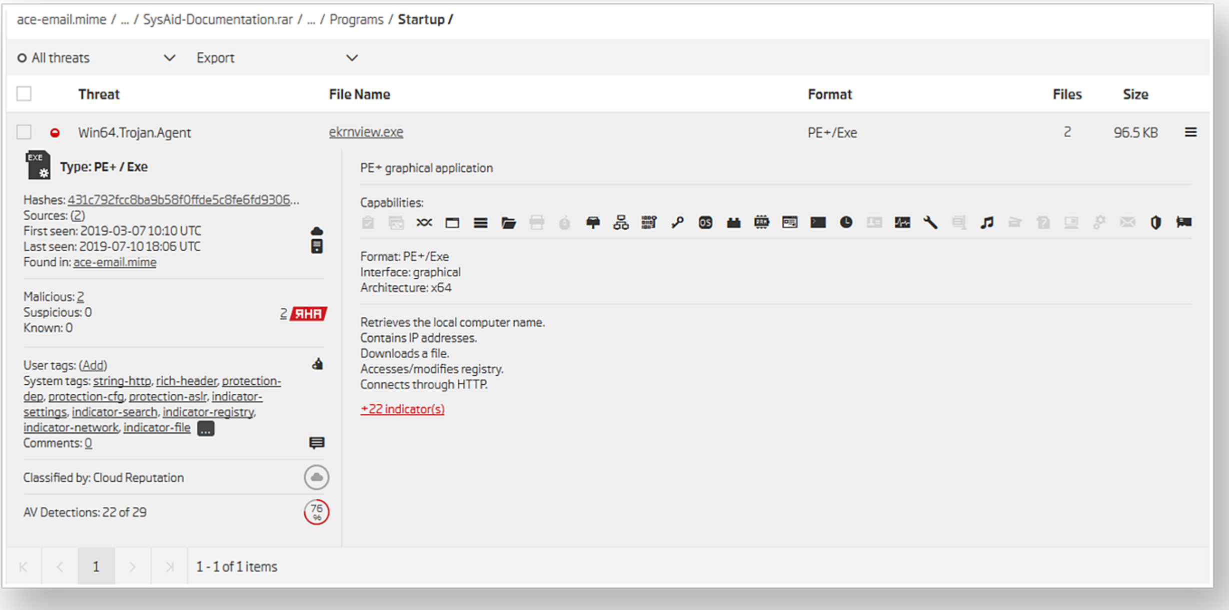
	Threat	File Name	Format	Files	Size
●	Win64.Trojan.Agent	ekrnview.exe	PE+/Exe	2	96.5 KB

1 - 1 of 1 items

Not only is the executable installed to the startup location, but it is also clear that this attack is a highly personalized one. The path traversal only works because the absolute paths are hardcoded to point to the user-specific startup folder. That makes the attack viable only for the machine of the intended email recipient, Idan.

At this point, it is clear that the attacker has compromised the organization. That Yosi's credentials are in the hands of the attacker. That the recon phase of the attack has been completed, and that the attacker is interested in moving laterally through the organization. It is more than likely that the next target, Idan, has access or information that the attacker is ultimately after.

The malicious executable the attacker expects to have successfully planted on Idan’s machine reveals more about the who and the why.



ace-email.mime / ... / SysAid-Documentation.rar / ... / Programs / **Startup /**

□	Threat	File Name	Format	Files	Size
□	Win64.Trojan.Agent	ekrnview.exe	PE+/Exe	2	96.5 KB

Type: PE+ / Exe

Hashes: 431c792fcc8ba9b58f0ffde5c8fe6fd9306...
Sources: (2)
First seen: 2019-03-07 10:10 UTC
Last seen: 2019-07-10 18:06 UTC
Found in: ace-email.mime

Malicious: 2
Suspicious: 0
Known: 0

2 ЯHA

User tags: (Add)
System tags: string-http, rich-header, protection-dep, protection-cfg, protection-aslr, indicator-settings, indicator-search, indicator-registry, indicator-network, indicator-file ...
Comments: 0

Classified by: Cloud Reputation

AV Detections: 22 of 29

76 %

PE+ graphical application

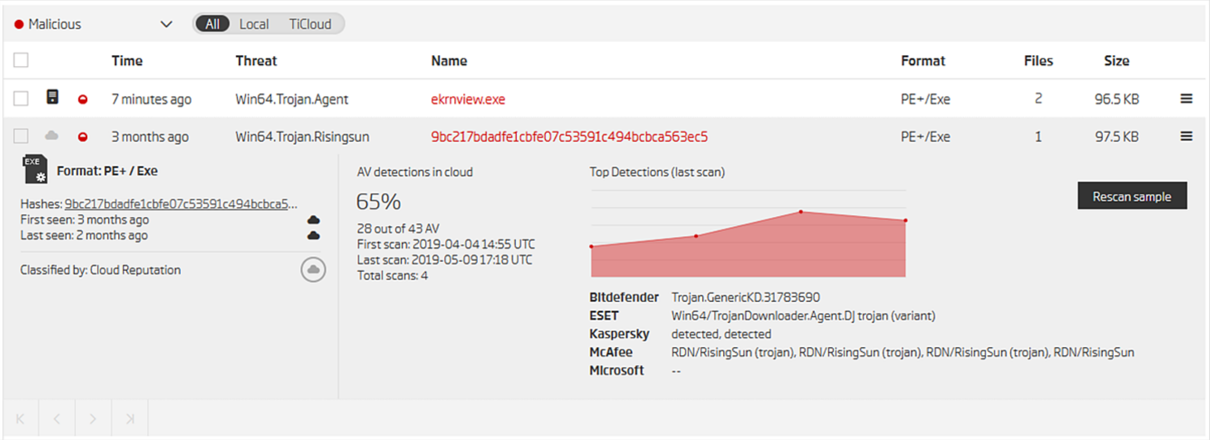
Capabilities:

Format: PE+/Exe
Interface: graphical
Architecture: x64

Retrieves the local computer name.
Contains IP addresses.
Downloads a file.
Accesses/modifies registry.
Connects through HTTP.

+22 indicator(s)

While "Agent" is not a particularly interesting or indicative threat name produced by our system, it is a starting point. It means that the threat itself isn’t particularly unique, and that it shares at least some of the commonality with previously discovered trojans. This is where functional code similarity can help. There is exactly one more file in the ReversingLabs cloud system similar to the one we’re looking at.



□	Time	Threat	Name	Format	Files	Size
□	7 minutes ago	Win64.Trojan.Agent	ekrnview.exe	PE+/Exe	2	96.5 KB
□	3 months ago	Win64.Trojan.Risingsun	9bc217bdadfe1cbfe07c53591c494bcbca563ec5	PE+/Exe	1	97.5 KB

Format: PE+ / Exe

Hashes: 9bc217bdadfe1cbfe07c53591c494bcbca5...
First seen: 3 months ago
Last seen: 2 months ago

Classified by: Cloud Reputation

AV detections in cloud

65%

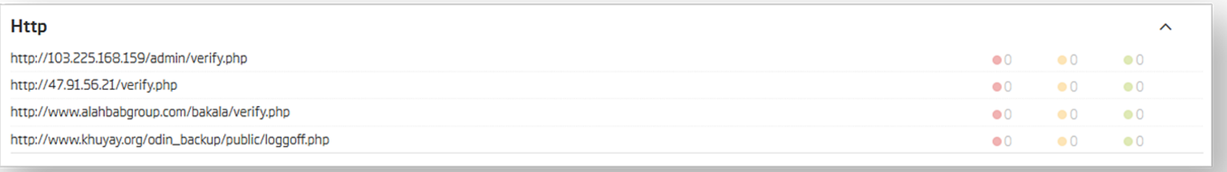
28 out of 43 AV
First scan: 2019-04-04 14:55 UTC
Last scan: 2019-05-09 17:18 UTC
Total scans: 4

Top Detections (last scan)

BItdefender	Trojan.GenericKD.31783690
ESET	Win64/TrojanDownloader.Agent.DJ trojan (variant)
Kaspersky	detected, detected
McAfee	RDN/RisingSun (trojan), RDN/RisingSun (trojan), RDN/RisingSun (trojan), RDN/RisingSun
MIcrosoft	--

That file has been classified as RisingSun Trojan by McAfee. The report which McAfee’s Advanced Threat Research team published on the Operation Sharpshooter describes what we’ve seen so far perfectly - an advanced attacker targeting the defense sector.

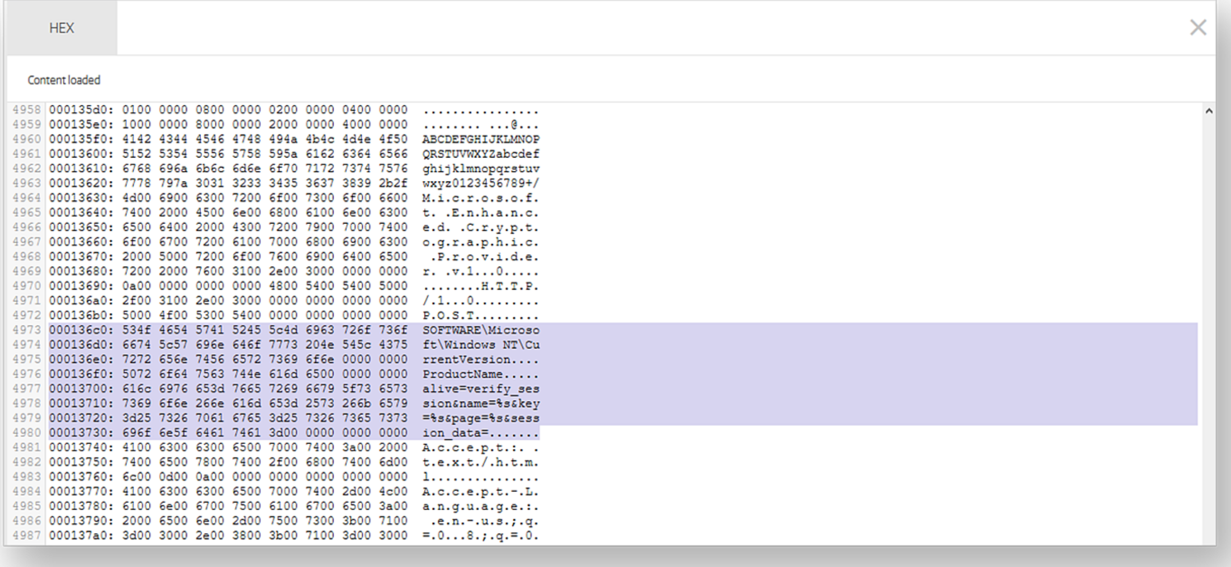
The suspicion that the attacks are connected is further supported by URLs extracted from the relevant executable. They seem to follow the same pattern as described in McAfee's report.



Http ^

http://103.225.168.159/admin/verify.php	● 0	● 0	● 0
http://47.91.56.21/verify.php	● 0	● 0	● 0
http://www.alahbabgroup.com/bakala/verify.php	● 0	● 0	● 0
http://www.khuyay.org/odin_backup/public/loggoff.php	● 0	● 0	● 0

A look at the executable hex dump also reveals a few striking similarities between the attacks.



```
000135d0: 0100 0000 0800 0000 0200 0000 0400 0000  ................
000135e0: 1000 0000 8000 0000 2000 0000 4000 0000  ........ ...@...
000135f0: 4142 4344 4546 4748 494a 4b4c 4d4e 4f50  ABCDEFGHIJKLMNOP
00013600: 5152 5354 5556 5758 595a 6162 6364 6566  QRSTUVWXYZabcdef
00013610: 6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
00013620: 7778 797a 3031 3233 3435 3637 3839 2b2f  wxyz0123456789+/
00013630: 4d00 6900 6300 7200 6f00 7300 6f00 6600  M.i.c.r.o.s.o.f.
00013640: 7400 2000 4500 6e00 6800 6100 6e00 6300  t. .E.n.h.a.n.c.
00013650: 6500 6400 2000 4300 7200 7900 7000 7400  e.d. .C.r.y.p.t.
00013660: 6f00 6700 7200 6100 7000 6800 6900 6300  o.g.r.a.p.h.i.c.
00013670: 2000 5000 7200 6f00 7600 6900 6400 6500   .P.r.o.v.i.d.e.
00013680: 7200 2000 7600 3100 2e00 3000 0000 0000  r. .v.1...0.....
00013690: 0a00 0000 0000 0000 4800 5400 5400 5000  ........H.T.T.P.
000136a0: 2f00 3100 2e00 3000 0000 0000 0000 0000  /.1...0.........
000136b0: 5000 4f00 5300 5400 0000 0000 0000 0000  P.O.S.T.........
000136c0: 534f 4654 5741 5245 5c4d 6963 726f 736f  SOFTWARE\Microso
000136d0: 6674 5c57 696e 646f 7773 204e 545c 4375  ft\Windows NT\Cu
000136e0: 7272 656e 7456 6572 7369 6f6e 0000 0000  rrentVersion....
000136f0: 5072 6f64 7563 744e 616d 6500 0000 0000  ProductName.....
00013700: 616c 6976 653d 7665 7269 6679 5f73 6573  alive=verify_ses
00013710: 7369 6f6e 266e 616d 653d 2573 266b 6579  sion&name=%s&key
00013720: 3d25 7326 7061 6765 3d25 7326 7365 7373  =%s&page=%s&sess
00013730: 696f 6e5f 6461 7461 3d00 0000 0000 0000  ion_data=.......
00013740: 4100 6300 6300 6500 7000 7400 3a00 2000  A.c.c.e.p.t.:. .
00013750: 7400 6500 7800 7400 2f00 6800 7400 6d00  t.e.x.t./.h.t.m.
00013760: 6c00 0d00 0a00 0000 0000 0000 0000 0000  l...............
00013770: 4100 6300 6300 6500 7000 7400 2d00 4c00  A.c.c.e.p.t.-.L.
00013780: 6100 6e00 6700 7500 6100 6700 6500 3a00  a.n.g.u.a.g.e.:.
00013790: 2000 6500 6e00 2d00 7500 7300 3b00 7100   .e.n.-.u.s.;.q.
000137a0: 3d00 3000 2e00 3800 3b00 7100 3d00 3000  =.0...8.;.q.=.0.
```

The email Yosi sent to Idan may very well be an indication of new activity for this APT actor. While the infection techniques seem to have evolved since McAfee published their report in December 2018, the methods of operation remained similar. The list of targets the actor is interested in has apparently been expanded to a new region as well - Israel.

Scouring the web for additional information based on what's been discovered at this point reveals one more report published by the FireEye Threat Research team. They go into the analysis of this same email, so it is recommended to read their report as a follow-up to our discussion here.

Email is an important threat-carrying vector. Securing an organization's email infrastructure mandates checking all emails received by the organization, whether they are coming from the outside or from within. The ReversingLabs Titanium platform enables such deep inspection with its elastic file processing capabilities. With our platform, the possibility of checking every email message the organization sees becomes the norm. Deploying such a capability within an organization could make the difference between catching the lateral email movement and missing it altogether.

IOC:
MIME - 5b5d7d74db59c520b72be1e328563a1ee864e8931a0ae7487d753ee3e166de1c

URL:
http://www[.]alahbabgroup[.]com/bakala/verify.php
http://www[.]khuyay[.]org/odin_backup/public/loggoff.php
http://103[.]225[.]168[.]159/admin/verify.php
http://47[.]91[.]56[.]21/verify.php

Read our prior blog in the series on Ransomware in exotic email attachments.

MORE BLOG ARTICLES