Gootkit banking Trojan jumps the Channel

First documented in mid-2014 [1], the Gootkit banking Trojan appeared to focus solely on customers from several French banks. This JavaScript-based malware combines web-injects (a la Zeus) and a clever persistence technique to create a robust tool for stealing online banking logins and other credentials from users of infected systems. In 2015, Gootkit integrated certain fileless features previously noted in Poweliks [2], and it has also been observed being dropped directly by Angler EK (Fig. 1) or indirectly via Bedep (Fig. 2).

#	Met...	Re...	Protocol	IP	Host	URL	Content-Type	Body
1	GET	200	HTTP	162.248.243.78	asd.baronlistertekki.biz	/ya8zwl6wn9	text/html	91 225
2	GET	200	HTTP	162.248.243.78	asd.baronlistertekki.biz	/6iVO06Y41YLP-YKvyL4hpJ4DnPDO8Aq1rNLH_037shXb6R...	application/x-shockwave-flash	76 984
3	**GET**	**200**	**HTTP**	**162.248.243.78**	**asd.baronlistertekki.biz**	**/2WkXmI5vGH00lbCvxR5kyLkIqnZwgNrVKhB7ueT...**	**application/octet-stream**	**234 897**
4	POST	200	HTTP	208.113.226.171	www.earthtools.org	/timezone/0/0	application/xml	496
5	POST	200	HTTP	23.201.216.11	www.ecb.europa.eu	/stats/eurofxref/eurofxref-hist-90d.xml	text/xml	76 311
6	POST	200	HTTPS	188.165.202.162	viqbatymsxdvz.com	/	text/html	60
7	**POST**	**200**	**HTTPS**	**188.165.202.162**	**viqbatymsxdvz.com**	**/**	**application/octet-stream;**	**212 992**
8	POST	200	HTTPS	188.165.202.162	viqbatymsxdvz.com	/	text/html	151 564
9	POST	200	HTTPS	188.165.202.162	viqbatymsxdvz.com	/	text/html	0
10	POST	200	HTTPS	188.165.202.162	viqbatymsxdvz.com	/	text/html	0
11	**GET**	**200**	**HTTPS**	**162.244.34.7**	**transferringcert.com:80**	**/rbody32**	**application/octet-stream**	**2 654 004**

(https://www.proofpoint.com/sites/default/files/figure-1.png)

Figure 1: Angler EK dropping Gootkit (2014-09-23)

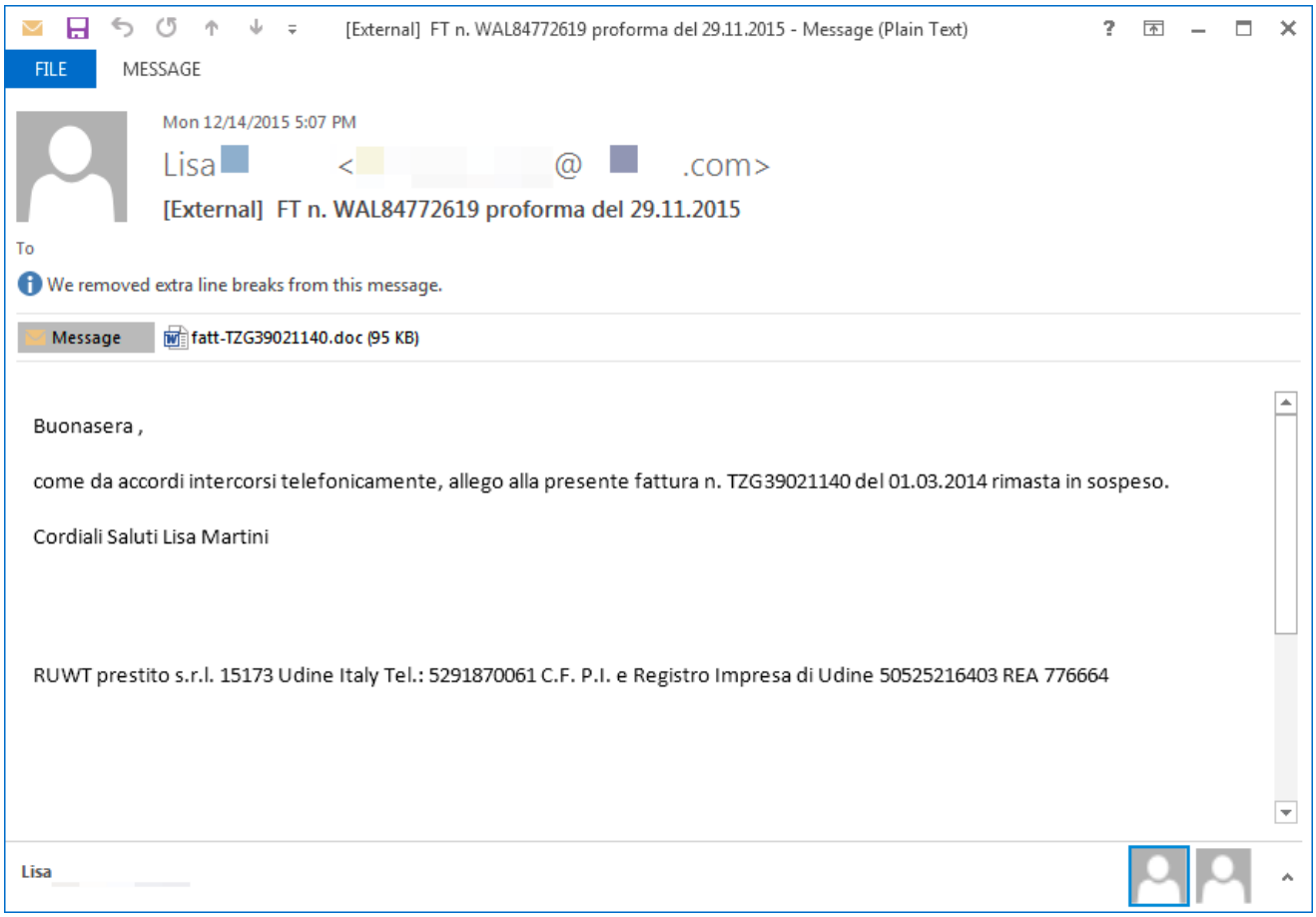
Met...	Re...	Protocol	IP	Host	URL	Content-Type	Body
GET	200	HTTP	131.72.136.235	qwe.yesterdayopenfour.biz	/2gdvinhy4d	text/html	70 592
GET	**200**	**HTTP**	**131.72.136.235**	**qwe.yesterdayopenfour.biz**	**/-VD0XlyIBNuZpTy6kwJv0f7nk1_339ptroqR1he7...**	**application/octet-stream**	**84 665**
POST	200	HTTP	208.113.226.171	www.earthtools.org	/timezone/0/0	application/xml	496
GET	**200**	**HTTP**	**131.72.136.235**	**qwe.yesterdayopenfour.biz**	**/m1rCPnSeriI5U1EuRVS8kph7Nq4dHGw5hoLavSf...**	**application/x-shockwav...**	**28 440**
GET	200	HTTP	131.72.136.235	qwe.yesterdayopenfour.biz	/RL_EgQL7C3xhmdNVD-1WkcY8X8WcjU0_RTMrw2-p-Bqq...	text/html	46 789
POST	200	HTTP	23.35.120.11	www.ecb.europa.eu	/stats/eurofxref/eurofxref-hist-90d.xml	text/xml	76 221
POST	200	HTTPS	209.126.97.209	aemmiphbweeuef59.com	/	text/html	60
POST	**200**	**HTTPS**	**209.126.97.209**	**aemmiphbweeuef59.com**	**/**	**application/octet-stream;**	**282 016**
GET	200	HTTP	131.72.136.235	qwe.yesterdayopenfour.biz	/9OuEVMvz12d5eWJuBmYXxg35Y3B7rWeU6jutIjz21xLxb...	text/html	0
GET	200	HTTP	131.72.136.235	qwe.yesterdayopenfour.biz	/yazajKn7oh7HpTsoZZqhV-aE_YaGahsdrky_sNw-Mwwjwu...	text/html	0
POST	**200**	**HTTPS**	**209.126.97.209**	**aemmiphbweeuef59.com**	**/**	**application/octet-stream;**	**520 204**
POST	200	HTTPS	209.126.97.209	aemmiphbweeuef59.com	/	text/html	0
GET	**200**	**HTTPS**	**31.148.220.186**	**spaceministrer.com:80**	**/rbody32**	**application/octet-stream**	**3 081 508**
GET	**200**	**HTTPS**	**31.148.220.186**	**spaceministrer.com:80**	**/rbody64**	**application/octet-stream**	**3 609 418**

(https://www.proofpoint.com/sites/default/files/figure-2.png)

Figure 2: Bedep dropping Gootkit (2014-12-10)

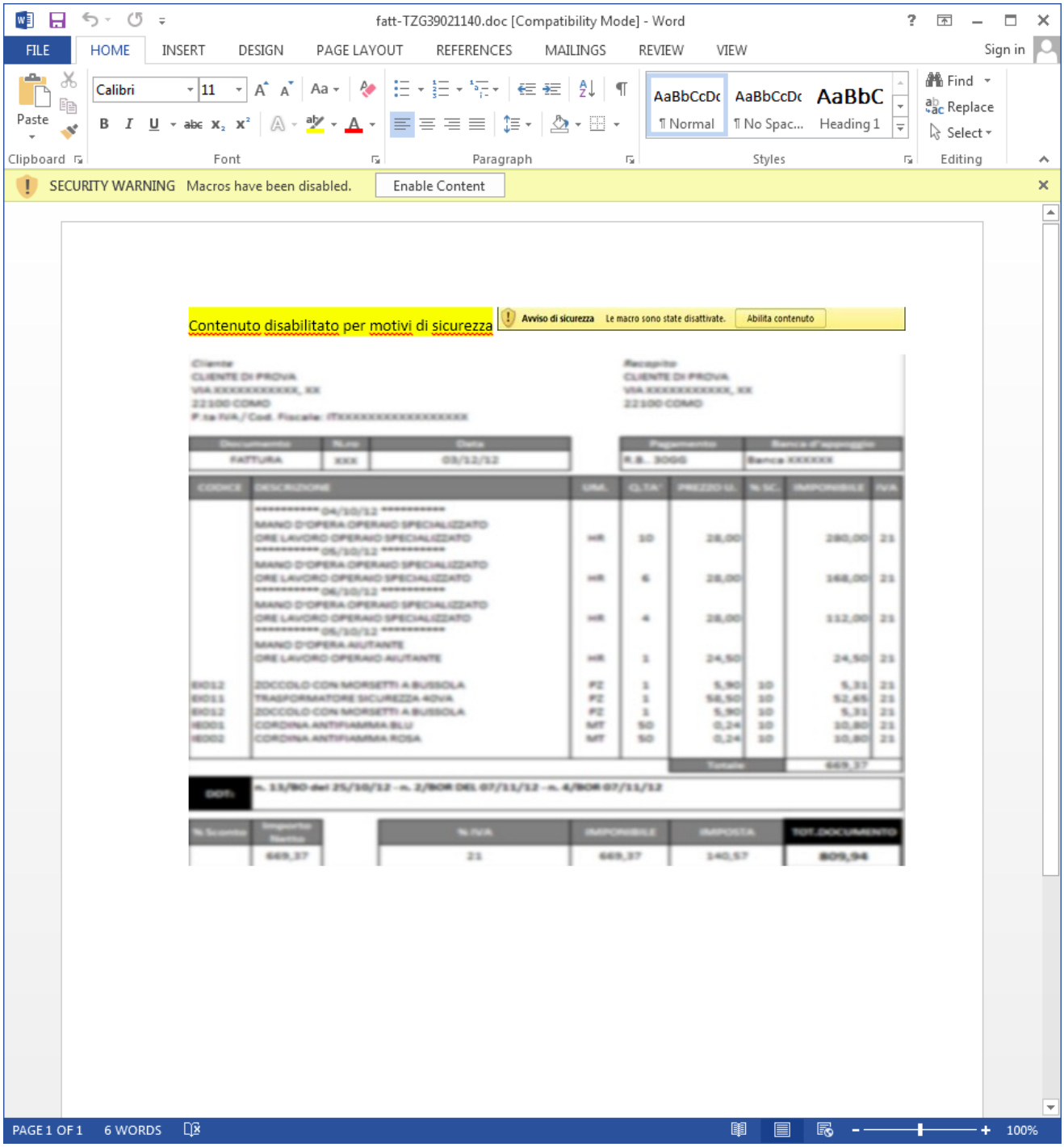
Gootkit has been observed targeting credentials for customers of a range of French financial institutions, including Crédit Mutuel, BNP Paribas, Le Crédit Lyonnais, Crédit Agricole, Société Générale, BTP Banque, and Crédit Coopératif. In March 2015, this distribution expanded to include customers of French and Italian banks through spam campaigns [3] that are still ongoing.

Here is an example of an email and accompanying Word doc used to deliver Gootkit to Italian targets in December of 2015.



(https://www.proofpoint.com/sites/default/files/figure-3.png)

Figure 3: Email used to deliver Gootkit (2015-12-14)



(https://www.proofpoint.com/sites/default/files/figure-4.png)

Figure 4: Word document used to deliver Gootkit (2015-12-14)

This expansion continued in late October, as Proofpoint researchers observed Gootkit being dropped by Angler EK through multiple infection paths in Canada. Since 2015-11-26, Gootkit has also been seen dropped in Great Britain via Angler EK at the end of a malvertising infection chain.

36	200	[redacted]	HTTP	GET	[redacted]	/lnkb.php	173	text/html; charset=UTF-8	0a8011937e14617ae54090bbb1eb4b82	Redirector After TDS
37	200	192.99.184.13	HTTP	GET	vip9tt.xfs2vmki.xyz	/boards/index.php?PHPSESSID=11v&action=45284ch75il8g06.l67	90 774	text/html	b3cf286b019801abeed1e6315b2e4dff	Angler EK
38	200	192.99.184.13	HTTP	POST	vip9tt.xfs2vmki.xyz	/boards/mark.pptmhtml?leach=NaIyhCkHP&manner=U7dDDW98poet=90db&...	2 384	text/html	3b96872b6141fc7c33e868af703f5cd9	Angler EK
39	404	192.99.184.13	HTTP	GET	vip9tt.xfs2vmki.xyz	/hope.docmhtml?speak=x0h&too=&talk=7qrU&captain=&save=eG0GLrhCU&...	0	text/html	No body	Angler EK
40	200	192.99.184.13	HTTP	GET	vip9tt.xfs2vmki.xyz	/hope.docmhtml?speak=x0h&too=&talk=7qrU&captain=&save=...	131 155	application/x-shockwave...	20701f56e487558a27bec774accff374	Angler EK : CVE-2015-7645
41	200	192.99.184.13	HTTP	POST	vip9tt.xfs2vmki.xyz	/wide.webarchivexml?reduce=lPG393Fx&stock=zGrRfgL&individual=zTX48&ke...	5 528	text/html	917d5b4723dbae8e446e070ef1db1a4b	Angler EK
42	200	192.99.184.13	HTTP	GET	vip9tt.xfs2vmki.xyz	/church.cms?to=&measure=VL41Gd0jb8&movement=rhazCU&rem...	295 948	application/octet-stream	a330852bb79648236c6c4e1828c7a128	Angler EK Payload
43	200	192.99.184.13	HTTP	GET	vip9tt.xfs2vmki.xyz	/meet.svc?concern=TJIte9-qhV&generally=0CNHZX&family=e5QE...	295 948	application/octet-stream	10fc3ed369a62c5a3d3edd0589bd01d7	Angler EK Payload
44	200	185.86.149.224	HTTPS	GET	babosikidai.com:80	/rbody320	4	application/octet-stream	3fb1dbc8331c15067d3f9a27375a6972	Gootkit Calling Home
45	200	185.86.149.224	HTTPS	GET	babosikidai.com:80	/rbody320	4	application/octet-stream	3fb1dbc8331c15067d3f9a27375a6972	Gootkit Calling Home
46	200	185.86.149.224	HTTPS	GET	babosikidai.com:80	/rbody32	3 072 546	application/octet-stream	87ed188af98f92c741a9585f2d121dad	Gootkit Calling Home
47	200	185.86.149.224	HTTPS	GET	babosikidai.com:80	/rbody32	3 072 546	application/octet-stream	87ed188af98f92c741a9585f2d121dad	Gootkit Calling Home

(https://www.proofpoint.com/sites/default/files/figure-5.png)

Figure 5: Gootkit dropped by Angler EK in Great Britain at the end of a Malvertising chain (2015-12-13)

```
div>\n            <div id=\"fake_message\" class=\"hide translatable\" data-translation=\"fake_message\">\n\t\t\t\tWe've detected
something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue,
we need to verify your identity with a security questions.\n            </div>\n            <div id=\"most_first_fake_message\"
class=\"translatable\" data-translation=\"fake_message_one\">\n                    It seems that you have not used the same device that you
used earlier. To ensure the security of your account, please answer a few questions.\n            </div>\n            <div
id=\"ff_fake_area_body\" class=\"hide\">\n                <!------------------------------ !! Message Error Start !!
---------------------------------------->       \n              <div id=\"error_verification\">\n                    <div
class=\"error_title\">\n                    <div class=\"error_message translatable\" data-
translation=\"error_message\">\n                    *** Your Challenge Response was invalid. Please verify your response and try
again!\n\t\t\t\t\t\t\t<div class=\"error_body translatable\" data-translation=\"error_body\">\n\t\t\t\t\t\t\t\tAttention:  Please review
the items below  to continue your application. ***\n\t\t\t\t\t\t\t</div>\n                                    </div> \n                    </
div>              \n              </div>\n \n \n <!------------------------------ !! Message Error End !!
----------------------------------------> \n \n <!------------------------------ !! Bank Card Start !!
----------------------------------------->\n \n              <div id=\"bank_card\" class=\"hide\">\n                    <div
id=\"bank_card_infront\" class=\"bank_card bc_infront\">\n                    <div
class=\"card_number\">\n                    <div class=\"bc_group\">\n                    <div
class=\"bc_group_title\">\n                    <label for=\"cc1\" class=\"translatable\" data-
translation=\"card_number\"> card number (16 digit)</label>\n                    </div>\n                    <div
class=\"row\">\n                    <input id=\"cc1\" class=\"card_num bc_block_size_75 required verifiable\" data-check-
pattern=\"[4-6]\\d{3}\" maxlength=\"4\" type=\"text\" value=\"XXXX\" placeholder=\"XXXX\"></input>\n                    <
input id=\"cc2\" class=\"card_num bc_block_size_75 required verifiable\" data-check-pattern=\"\\d{4}\" maxlength=\"4\" type=\"text\"
value=\"XXXX\" placeholder=\"XXXX\"></input>\n                    <input id=\"cc3\" class=\"card_num bc_block_size_75
required verifiable\" data-check-pattern=\"\\d{4}\" maxlength=\"4\" type=\"text\" value=\"XXXX\" placeholder=\"XXXX\"></
input>\n                    <input id=\"cc4\" class=\"card_num bc_block_size_75 required verifiable\" data-check-
pattern=\"\\d{4}\" maxlength=\"4\" type=\"text\" value=\"XXXX\" placeholder=\"XXXX\"></input>\n                    </
div>\n                </div>\n                </div>\n                <div
class=\"expiration_date\">\n                <div class=\"bc_group\">\n                    <div
class=\"bc_group_title\">\n                    <label for=\"expmm\" class=\"translatable\" data-
translation=\"expiration_date\"> expiration date</label>\n                    </div>\n                    <input
id=\"expmm\" class=\"bc_block_size_75 required verifiable\" data-check-pattern=\"01|02|03|04|05|06|07|08|09|10|11|12\" maxlength=\"2\"
type=\"text\" value=\"MM\" placeholder=\"MM\"></input>\n                    <input id=\"expyy\" class=\"bc_block_size_75
required verifiable\" data-check-pattern=\"20(15|16|17|18|19|20|21|22|23|24|25|26|27|28|29)\" maxlength=\"4\" type=\"text\"
value=\"YYYY\" placeholder=\"YYYY\"></input>\n                    </div>\n                    </div>\n                    </
div>\n                <div id=\"bank_card_behind\" class=\"bank_card bc_behind\">\n                    <div
class=\"bc_cvv_info\">\n                    <div class=\"bc_group translatable\" data-
translation=\"cvv_or_cvc\">\n                    CVV or CVC - 3 digit code on back of the card\n                    </
div>\n                </div>\n                <div class=\"cvv\">\n                    <div
class=\"bc_group\">\n                <div class=\"bc_group_title\">\n                    <label
for=\"cvv\" class=\"translatable\" data-translation=\"cvv\">CVV/CVC</label>\n                    </
div>\n                <input id=\"cvv\" type=\"text\" class=\"bc_block_size_60 required verifiable\" data-check-
pattern=\"\\d{3}\" maxlength=\"3\" value=\"XXX\" placeholder=\"XXX\"></input>\n                    </
div>\n                </div>\n                </div>\n                </div>\n \n <!------------------------------ !! Bank
Card End !! ----------------------------------------->\n\n\n <!------------------------------ !! Question Lists Start !!
----------------------------------------->\n                <div id=\"question\" class=\"hide\">\n                    <div
```

(https://www.proofpoint.com/sites/default/files/figure-6.png)

Figure 6: Snippet of UK-focused injects tied to sample 58aeefd4700af5cb1db1f5603025a5ec

Configs from the UK-focused injects (Fig. 6) show that these latest payloads are attempting to capture information from customers of a range of financial institutions that are based or operate in the UK, including Paypal, Santander, Natwest, Ulster Bank, Royal Bank of Scotland, and Barclays.

This expanded targeting follows a trend we have observed in recent months, as threat actors seek to reach new victims by shifting their distribution to new regions and verticals. With Gootkit finally crossing the Channel it would not be surprising to see it in other regions in the near future, as well as to see other malware with limited geographic presence (such as Shifu) jump on this trend.

References

[1] Analyzing Gootkit's persistence mechanism (new ASEP inside!) - 2015-04-13 - CERTSG - http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html (http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html)

[2] Win32/Xswkit (alias Gootkit) - http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3669 (http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3669)

[3] Fake Judicial Spam Leads to Backdoor with Fake Certificate Authority - 2015-03-30 - http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/ (http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/)

[4] “Hey Brian, Heya Homer, fancy meeting you here!” – Zeus Gootkit, 2014 AD - 2014-08-07 - CertLexsi https://www.lexsi.com/securityhub/hey-brian-heya-homer-fancy-meeting-you-here-zeus-gootkit-2014-ad/?lang=en (https://www.lexsi.com/securityhub/hey-brian-heya-homer-fancy-meeting-you-here-zeus-gootkit-2014-ad/?lang=en)

Indicators of Compromise (IOC’s)

File hashes:

6195950991475ec363f53b2c570469512b8e4a1995db73056cff39251c211dff - 2015-08-26 - CAN

a24c9996913ecbe2af183e5ac3d176f869ed62e15a31deb2dc2ea947900432c3 - 2015-11-26 - GBR

cb55bd4ee66ee8fcbda9f0f15192406bb1d089bc72a0f121395fafc8e04cb0e8 - 2015-12-02 - CAN

532bd85487ce3c16654d21c6425f6f728430d50e47e802b332ea82ae0511adca - 2015-12-13 - GBR

3922F2317BE8D0420F1DC938A633B3243D938FC0098A528D70B89C2D2F080C5C - 2015-12-21 - ITA

C2 server addresses:

swysocki77.com - 138.204.171.103

gorski83.com

ostrowski87.com

jasinski2015.com

olszewski78.com

pozheeshebudem.com

freforevermailtes.com

nidermidertom.com

ecuremailbestfree.com

securewebgooglesite.com

robertpouslen12494.pw - 151.80.201.187

robertpouslen1234524.com

update-service7825t28.com

domolor.com - 108.61.178.212

babosikimne.com - 81.2.241.227

babosikidai.com - 185.86.149.224

vaillantsawer.com - 198.96.89.181 185.82.202.38

proballansmen.com

reputamadrell.com

lastrizariano.com

rokobarokkino.com

artipreambulo.com

trequablaster.com

pretriquestro.com

rebellintosto.com

mellicianactr.com

abc.doitgraphic.org - 198.71.232.3
updatebase.bid
shop.lifexcellence.org

ET Open and Pro rules:

2022257 || ET TROJAN Possible Gootkit CnC SSL Cert M5

2022256 || ET TROJAN Possible Gootkit CnC SSL Cert M4

2022255 || ET TROJAN Possible Gootkit CnC SSL Cert M3

2022253 || ET TROJAN Possible Gootkit CnC SSL Cert M1

2019907 || ET CURRENT_EVENTS Gootkit SSL Cert Dec 10 2014

2022259 || ET TROJAN Possible Gootkit CnC SSL Cert M7

Tuesday, December 22, 2015 - 19:00

- Press Releases > (http://blog.proofpoint.com/us/news/press-releases)
- Proofpoint in the News > (http://blog.proofpoint.com/us/news/in-the-news)
- Proofpoint Blog > (http://blog.proofpoint.com/us/news/blog)
- Threat Insights blog > (http://blog.proofpoint.com/us/threat-insight)
- Events > (http://blog.proofpoint.com/us/events)
- Media Contacts > (http://blog.proofpoint.com/us/contact-us)

ADD NEW COMMENT

Your name

Subject

Comment *

Switch to plain text editor

More information about text formats (/us/filter/tips)

Text format

Filtered HTML

- Allowed HTML tags: <cite> <blockquote> <s> <sub> <sup> <i> <b>   <u> <a> <p>
 <img>

Save Preview

BACK TO TOP

SOLUTIONS

FOR YOUR NEED

Threat Protection (/us/solutions/needs/threat-protection)
Detect, classify, and respond to threats

Compliance (/us/solutions/needs/compliance)
Control and encrypt your data, share securely, and prevent data loss

Discovery (/us/solutions/needs/discovery)
Cloud archiving, governance, and discovery

FOR YOUR ROLE

Security (/us/solutions/role/security)

Messaging Ops (/us/solutions/role/messaging-ops)
Legal (/us/solutions/role/legal)
Compliance (/us/solutions/role/compliance)

FOR YOUR INDUSTRY

Education (/us/solutions/industry/education)
Financial Services (/us/solutions/industry/financial-service)
Government (/us/solutions/industry/government)
Healthcare (/us/solutions/industry/healthcare)
Manufacturing (/us/solutions/industry/manufacturing)
Pharmaceutical (/us/solutions/industry/pharmaceutical)
Retail (/us/solutions/industry/retail)

FOR YOUR APPLICATION

Office 365 (/us/office365)
Social Apps (/us/solutions/application/social-media)

PRODUCTS

FOR SMALLER BUSINESS

Proofpoint Essentials (/us/solutions/smb/proofpoint-essentials)
Proofpoint Essentials Support (http://support.proofpointessentials.com/)

ENTERPRISE PRODUCTS

Enterprise Protection (/us/solutions/products/enterprise-protection)
Targeted Attack Protection (http://proofpoint.com/solutions/products/targeted-attack-protection)
Threat Response (/us/solutions/products/threat-response)
Privacy, DLP and Encryption (/us/solutions/products/enterprise-privacy-suite)
Malvertising Protection (/us/solutions/products/malvertising-protection)
Archive (/us/solutions/products/enterprise-archive)
Governance (/us/solutions/products/enterprise-governance)
Content Control (/us/solutions/products/content-control)
Sentrion Sendmail (/us/solutions/products/sentrion-sendmail)
Social Media Security (http://nexgate.com)
TAP Mobile Defense (/us/solutions/products/tap-mobile-defense)

BLOGS, NEWS, EVENTS

Threat Insight (/us/threat-insight)

News (/us/news)
Events (/us/node/1708)
Corporate Blog (/us/corporate-blog)

INFORMATION

Partners (/us/partners)
Service & Support (/us/services/support-services)
Investors (http://investors.proofpoint.com/)
Careers (/us/careers/life-proofpoint)

WHY PROOFPOINT

Cloud and Big Data Platform (/us/why-proofpoint/cloud-big-data)
Satisfied Customers (http://proofpoint.com/us/customer-stories)
About Us (/us/why-proofpoint/about-us)

Call (/us/contact-us)
Email (/us/contact-us)
Chat
Request Demo (/us/request-free-trial-or-demo-proofpoint-security-and-compliance-solutions)

REGIONS

United States (/us)
United Kingdom (/uk)
France (/fr)
Germany (/de)
Spain (/es)
Japan (/jp)
Taiwan (/tw)
Australia (/au)

PARTNER LOG-IN (/us/partner-log)

SENDMAIL SUPPORT LOG-IN (https://www.sendmail.com/cfusion/CFIDE/smi/support/)

SUPPORT LOG-IN (https://support.proofpoint.com/)

PRIVACY POLICY (/US/PRIVACY-POLICY)