El Machete's Malware Attacks Cut Through LATAM

cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html

The BlackBerry Cylance Threat Research Team

RESEARCH & INTELLIGENCE / 03.22.17 / The BlackBerry Cylance Threat Research Team

Executive Summary

The SPEAR™ Team has once again jumped back into tracking and monitoring threats following public disclosure, to discover what happens next. What we've found is that the current barrier to bypass existing defense solutions is so low that attackers need only make very minor changes to continue to use publicly disclosed malware effectively. El Machete is one of these threats that was first publicly disclosed and named by Kaspersky here. We've found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in order to evade signature-based detection.

SPEAR was able to identify just over three hundred unique victims over the past month, as well as over 100GB worth of data that was exfiltrated and stored on one of the C2 servers. The bulk of the victims were predominantly based out of Ecuador, Venezuela, Peru, Argentina, and Columbia; however, other victims were identified in Korea, the United States, the Dominican Republic, Cuba, Bolivia, Guatemala, Nicaragua, Mexico, England, Canada, Germany, Russia, and Ukraine. Targets included a wide array of high-profile entities, including intelligence services, military, utility providers (telecommunications and power), embassies, and government institutions.

Perhaps what's most interesting in the current dataset is that the majority of countries that were most heavily targeted share a land border with Brazil. However, SPEAR did not identify any Brazilian victims, contrary to Kaspersky's initial findings.

Findings

Phishing emails continued to use links to external ZIP or RAR archives, which ultimately contained an executable with the extension SCR. All of the executables SPEAR identified contained either an executable generated by the open source Nullsoft Scriptable Install System (https://sourceforge.net/projects/nsis/) or a self-extracting RAR executable (SFX). NSIS provides a surprisingly easy way for attackers to obfuscate malicious code via multiple common compression routines like ZLib, BZip2, LZMA. The attackers also made extensive use of Hostinger's cheap web hosting services to deliver initial payloads. SPEAR identified the following URLs were used in phishing attempts:

hxxp://actualizacion.esy[dot]es/Mision_Secreta_de_la_DINA_en_Washigton.rar
hxxp://almuerzowordaula3.16mb[dot]com/ORDENES_GENERALES.rar
hxxp://carolinaz25.esy[dot]es/DECRETO_No_18_Duelo_Virgilio_Godoy_.rar
hxxp://carolinaz25.esy[dot]es/RDGMA_07_4432.rar
hxxp://cristianoo.esy[dot]es/Padrino_Lopez_Hay_un_golpe_de_Estado_en_desarrollo.zip
hxxp://cristianoo.esy[dot]es/ROSARIO_EN_MULTINOTICIAS_13_ABRIL_2016.zip
hxxp://flipjbl.esy[dot]es/Suport/Articulo%20sobre%20funcionarias%20de%20Nicaragua%20docx.rar
hxxp://flipjbl.esy[dot]es/Suport/Debes%20utilizar%20una%20computadora%20para%20extraer%20el%20contenido.rar
hxxp://informesanddocumentos.esy[dot]es/semanario_en_marcha_1758_1.zip

SPEAR observed the following filenames were used for malicious payloads delivered via social engineering techniques:

Payload Filenames:

977_REG_IN_CO_012_V1.scr
Aniversario_de_cascos_azules_ecuatorianos.docx.scr
Articulo sobre funcionarias de Nicaragua docx.scr
Articulo_de_Opinion_Heinz_Dieterich.docx.scr
Boletín_PAT_034_UADMNE_Visita_de_Guardianes_del_Mar_a_repartos_navales.scr
Citacion Judicial expediente 10388-17 Oficio 35467pdf.scr
CIRCULAR_8_OCT_2016.scr
Cuestionario.scr
DECRETO_No_18_Duelo_Virgilio_Godoy_.docx.scr
Demanda.scr
Denuncia_penal_o_querella.scr
DIRECTIVA_MANDO_OPERACIONAL.scr
Informe Derechos Humanos en Nicaragua docx.scr
INSTRUCTIVO LOGISTICO.scr
Jungmann verifica o funcionamento do SISFRON, em Dourados (MS).docx.scr
LISTA DEL RADG N° 0931208.scr
Ministerio_de_Defensa_ordena_al_Issfa_que_no_suspenda_tres_prestaciones.scr
Mision_Secreta_de_la_DINA_en_Washigton.scr
Nicaragua denuncia ante la CIJ las.scr
Notificacion_Judicial_No_121523_2015.scr
Notificacion_Judicial_No_121523_2016.scr
Notificacion_Judicial_No_8030923_2015.exe
ORDENES_GENERALES.scr
Padrino_Lopez_Hay_un_golpe_de_Estado_en_desarrollo.scr
PARTE ESPECIAL COMANDANCIA GENERAL DE LA AVIACIÓN 20SEP15.scr
RDGMA_07_4432.scr
REINCORPORACION.SCR
ROSARIO_EN_MULTINOTICIAS_13_ABRIL_2016.scr
Semanario_En_Marcha_1756_11.scr

The group still preferred to use PY2EXE to encode Python scripts to executables and relied on multiple compiled scripts to perform a number of different functions, including screen capture, video capture, audio capture, file enumeration, keystroke logging, and data exfiltration. As far as SPEAR could tell, all scripts were designed to be executed using Python v2.7. No other versions of the interpreter were identified. The group relied heavily on TLS-encrypted FTP using Python's native ftplib library to transfer data out of target environments. SPEAR only observed this activity over the usual TCP port 21. The samples would also test connectivity to the C2 via HTTP requests using Python's urllib library. An example request is shown below.

GET / HTTP/1.0
Host: idrt.gotdns.ch
User-Agent: Python-urllib/1.17

Figure 1: Sample Connectivity Request

The scripts themselves could be easily extracted and decompiled out of the binaries using uncompyle. The decompiled scripts employed some visual obfuscation techniques by naming variables as combinations of the characters 'o', 'O', and '0' to hinder analysis. One of the external modules was designed to find, encrypt, and upload files from fixed and removable drives using a predefined list of extensions; perhaps most interesting in this list was the inclusion of several graphical information systems file formats (GIS), as well as PGP/ GPG files and private key rings. In-depth analysis of the scripts showed the group employed AES in CBC mode using a predefined static key to encrypt files before uploading them to the C2 server. Several simple obfuscation measures, including various XOR encoding schemes, were employed by the malware to obscure configuration files, which was somewhat surprising given the use of stronger encryption used in exfiltration of important data.

The attackers appeared to prefer to use free dynamic DNS domains that provided No-IP or Command and Control (C2). SPEAR discovered the following domains and IP addresses were used continuously over the past two years:

Domains:

derte.ddns[dot]net
idrt.gotdns[dot]ch
jristr.hopto[dot]org
wbgs.3utilities[dot]com

IP Addresses:

176.9.3.184
213.239.232.149
69.64.43.33

The domain 'jristr.hopto[dot]org' shared a direct link to past El Machete activity via the IP address '181.50.98.50', which was also previously used by 'java.serveblog[dot]net'.

Persistence:

SPEAR found that El Machete relied on two primary means to achieve persistence: scheduled tasks and the startup folder. Scheduled tasks commonly used 'HD_Audio', 'Java_Upda', or 'Microsoft_up' as the task name and generally pointed to one of the executables below:

- %AppData%\Desjr\jfxrt.exe
- %AppData%\unijr\kfxw.exe
- %AppData%\MicroDes\javaH.exe

The path '%UserProfile%\Start Menu\Programs\Startup\Java Update.lnk' was used in one sample in 2015. 'HD Audio.lnk' was observed as a possible value in one of the decompiled scripts, however, the Startup Folder technique seems to have been largely abandoned in later samples, perhaps as a result of disclosure.

File-based Indicators:

The group preferred to create their own directories to drop files into, including:

- %AppData%\unijr\
- %AppData%\HDA\Bush\
- %AppData%\jre8\lib\
- %AppData%\java.\

- %AppData%\MicroDes\

For the sake of brevity, SPEAR has excluded all of the possible file names, but they should be readily accessible via the hashes provided below. The principal droppers were commonly SFX archives and were typically named either ‘jsx.scr’ or ‘RAVBg.scr’. Defenders should be wary of any script interpreters such as ‘python27.dll’ located in unusual directories.

Conclusion:

El Machete has continued largely unimpeded in their espionage activities for the past several years, despite the abundance of publicly available indicators. Many of these indicators should have allowed defenders to reliably identify this threat, but the majority of antivirus (AV) solutions continue to have very low detection rates across current samples. Compiled scripts are an increasingly complicated area of detection for security companies and will likely continue to be adopted by both skilled and unskilled attackers alike. Scripting languages natively provide an easy means of developing cross platform compatibility for other operating systems like OSX and Linux, however, all of the scripts SPEAR found appeared to be heavily reliant upon Windows APIs to perform critical functions.

El Machete will no doubt continue to be successful across most Latin American countries as they struggle to build up both their offensive and defensive cyber capabilities. Many of the targeted countries were listed as customers in the leaks of both Finfisher and Hacking Team, which suggests they likely have yet to fully mature and develop their own internal cyber capabilities. In any case, whoever is behind El Machete is certainly reaping the rewards of building and deploying their own custom malware.

If you use our endpoint protection product, CylancePROTECT®, you were already protected from this attack. If you don't have CylancePROTECT, contact us to learn how our AI based solution can predict and prevent unknown and emerging threats.

Appendix:

Zip Files:

a8f0a470d5365c58e8cdfe8b62d5b11e4fc0197731695868c583fc89b19ef130
6ba72f5c88f3253c196fc4e5c0b41c2b5dfba9456ce7e8393c4a36fdfc1c6add
3e08e7f85c1185a1583955f9efa247addef11991beb36eb8b3f89c555707575e
f7107b9fdba48cefeff824f45b7268dd083accc847836f16dae740ce3d3d6543
55ac70ec30269428626ba3c9433b4c9421712ec1a960b4590247447f45f26ac4

RAR Files:

048d43882bd7e55a245f11931f577e7ec706f2d64ba37c3372bc73f6971dc233
6d73387c8c132c8bfbc7a644524b4995cdb3b4c8700a8f12921bcb0f9b573ede
601587809f2da4b6bdfa8fdab087209bfe9555e68f34d9c0ba18a2a76eecfdb3
2265ad57ec790a239eea12af5398819cab744fe167142346055b36a32482e06e
27443b0e1864cee5ad787ec6dcdd4521186163b090278ddb4f75c35d0f52864e

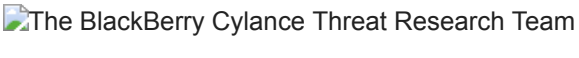
Initial Payload With Decoy:

06ae08f9628f40a75a01c266caaa440ec664c3138f9fd39b273e6d8c9ec50f17
0970e43cf5458b0cf77e2232f724a651e9f37513f5cb3c58b51d357c21e18e4c
0ebdf2390584d1c66dc908bd8b95c96673428c1c22fb495075b4c79e2f54f796
1661fb2e2b4f701203bf22b3cf339cc12f5779999ee1ced6818e5087714b074c
17236e97e665a0766be612e57a90332e86e44d18f31ccd2beb7487cfdfd2bb8f
1a5dcc6e43aac2f1fdf0928d817ef5358ba5420fc578f5ec3fa4fbd304d02f36
1d1dc7fe128330558f071aebdd9a6ee76ac24fd0009661f90ae8dc9ce8ec10d1
495aa2ac2c666e82c7244a74ac025006c3476f348105253adef7a225f98aeba1

4c14f7e1323a26d00cc9bf516ae1137a97e84691e4c2f525b16828e217ff037c
58207b19c327b3590c92279006458356249f929c71cdb18791b498dd08f36cc8
6b8a536740e8e5af9b472f90925856eb44e272f88a90ecaad1714576dae83f88
6bc30bd07cfbf20051057483b9883925bd4eda545376a793286e2d5315389181
6c60ff5e52c5b77012de3e43a1ba88b6c952e51b98d9651ddd6791c4af4a6607
7567935a0e3882278455f4b6e434021d6bdee51be56d455ce1a13e13fe28cdcd
82ee78877adeb3db055d924cc08148db03f7b6d4734b7deb2f59ab37269ffeb4
8434227d1db2679a36d767e7b0ffa5934496d947f4dcd765961d539108534df8
89e2bf8e057e5e5c1d99e5c533cc0352f4f86dd9bea03aae01b8c02454eed7a7
9641553bfdffbeb4e786f36ed9fc6545d6b8c624eddb576cc234ab43d4afff2a
acb60ec5dc7778fd4ab1f21bd9a406c04455f8d28b1e01e97bd0ac036d1e72e2
bba13073badce1669d858955613c4e10adf6d4577a517a618009bde93639d47a
c5278dabf24ecf9207ad8ee4ac3a4dd087ed3d671983c84c0babfc94a52da182
eab46451c053b6a606655a69c381a56a9afca4bf1bd2882c7c030ae69f892da7
ec2ac42b822de3ef7ec5c980075fd32ef134bf2fd31bfd368c563faee5702b60
f258d903d23e34b6109294e4ca3d18078652dea23eea13f77f496303d6798995
fa97b9f4d1f5f401f8bdb4c989d10e1c4d7f76e65a31a3b9ac34c10c17653a64
ffba9c46c2b991dabfa3b1e3d91dc4b4126086ba288b594836936145e9a8454b
d21d981bc5efba11e8abf17cd369045d3eefa5268d7457bce5136e399bedb241

Primary Droppers:

0972e075b70ea6f43b4a6f2c5e7f9329c3f4b382d7327b556131587142a3751f
14e3053393d9b3845cec621cd79b0c5d7cd7cf656be0f5a78bb16fd0439c9917
1c0f253b91b651e8cb61ea5dc6f0bf077bec3ab9612e78f9a30c3026e39bf8a8
28131cea5009f680064a7962279ebdff7728463a6d0a30ef2077999abe27bee7
282651843b51a1c81fb4c2d94f319439c66101d2a0d10552940ede5c382dc995
2f878a3043d8f506fa53265afcea40b622e82806d1438cf4a07f92fb01d9962f
3b326f99ce3f4d8fa86135a567ba236fcc0eb308cd5bbfc74404a5fe3737682a
52cec92c27d99c397e6104e89923aa126b94d3b1cf3afa1c49b353494219162e
5fed1bda348468eddbdd3cdefd03b6add327ff4d9cf5d2300201e08724b24c9a
613351824cabdb3932ab0709138de1fcff63f3f8926d51b23291ebf345df4471
6917db24c61e6de8be08d02febe764fe7e63218b37e4a22e9d7e8691eee38dcb
732ceaf2ce6f233bb4a305edc8d2bb59587a92bd6f03ea748bef6dd13bf38499
76af6661f95bf45537c961d4446d924a70b9b053ddbf02c8bfda2918d5ac90f5
93348d6dffd45a4c01b10fc90501c666f7a5360547e2a025d5980f235e815cc9
9d124733378333e556d29684eb05060e8c88eb476a5803d0879c41f4344f6bd9
b8341d72c3b2ecd90a18d428a7ea81a267eb105a36692042fe8904b0b0ea6b07
bc3cedfa6a2c05717116b29c2b387a985a504a97ce0e0a43212b3bc89ac9cf95
c634f10a475df833c55610e38e947dda278b474b6650bb8570ab3801be43739f
d2b81d32ceb61640c72d2af241527e942218e2067c7a0ae4ff5b6eabe659255e
f98ef639797013d6eddfcc00f7d208510ac02ca49bed1eb9250156081d5ed0ab



About The BlackBerry Cylance Threat Research Team

The BlackBerry Cylance Threat Research team examines malware and suspected malware to better identify its abilities, function and attack vectors. Threat Research is on the frontline of information security and often deeply examines malicious software, which puts us in a unique position to discuss never-seen-before threats.

Back