Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE APT DESCONOCIDO EN GUATEMALA

11/12/2023

CONTENIDO

INTRODUCCIÓN

El 27 de noviembre del presente año se descubrió sobre un ataque ATP Desconocido en Guatemala.

ATAQUE APT DESCONOCIDO EN GUATEMALA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_12_11_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/12/2023
Es día cero (0 day):	No

GENERAL

Los ataques informáticos han alcanzado proporciones alarmantes, desencadenando una crisis global de ciberseguridad que afecta a empresas, organizaciones gubernamentales y usuarios individuales en todo el mundo.

En las últimas semanas, se ha observado un aumento vertiginoso en la cantidad de ataques ciberneticos, en la región, una forma de malware que cifra los archivos de las víctimas y exige un rescate a cambio de la clave de descifrado. Estos ataques afectan a una amplia variedad de sectores, desde la atención médica hasta la industria manufacturera, dejando a las organizaciones paralizadas y causando estragos en la economía digital.

El 27 de noviembre del presente se descubrió sobre un ataque ATP Desconocido en Guatemala.

El ataque afecto plataformas críticas. Se observo que el vector de Initial Access (TA0001), se dio al vulnerar una aplicación web publica, en la cual se instaló un WebShell, llamada reGeorg.

Las vulnerabilidades informáticas en aplicaciones publicadas sin parchear representan una seria amenaza, ya que los atacantes pueden detectar las falencias de estas aplicaciones, ya que las vulnerabilidades más conocidas se encuentran de manera pública en internet.

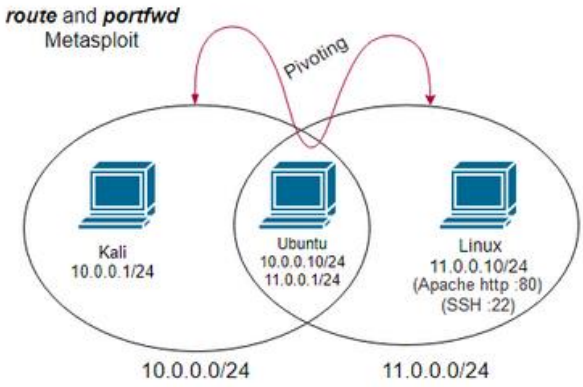
Las consecuencias de no abordar las vulnerabilidades informáticas son significativas. Los ataques pueden variar desde la manipulación de datos hasta la toma de control completa de un sistema. Además, los datos sensibles, como información personal, financiera o empresarial, pueden quedar expuestos, lo que pone en riesgo la privacidad y la confianza de los usuarios. La gestión adecuada de parches y actualizaciones es esencial para mitigar estas amenazas.

ReGeorg, el cual es utilizado para pivotear e intentar llegar a otros servicios o servidores de la red interna. Para ello se suele realizar un túnel para reenviar tráfico TPC sobre HTTP. ReGeorg (llamada reDuh hasta 2014), levanta un Proxy SOCKS4/5, y utiliza el módulo urlib3

La técnica de reGeorg se basa en el uso de un script JavaScript (regeorg.js) que se inyecta en una página web. El script permite establecer una conexión de ida y vuelta a través del firewall, gracias al uso de técnicas de tunelización HTTP. Esto significa que el tráfico se envía como solicitudes y respuestas HTTP legítimas, lo que facilita su paso a través de firewalls y sistemas de filtrado que solo permiten tráfico HTTP.

Cuando ya se ha establecido la conexión entre la máquina del atacante y el servidor objetivo, el atacante puede utilizar una herramienta, como proxychains, para pivotar su tráfico a través de la red del servidor.

Proxychains es una herramienta que permite enrutar el tráfico de red a través de múltiples proxies de forma transparente. El atacante configura proxychains para usar el túnel establecido con reGeorg como proxy, de modo que puede acceder a otros sistemas dentro de la red restringida a través del servidor objetivo.



Algunos de los IOCs detectados en el análisis son:

IOCs Detectados

Archivos usados para respaldar las operaciones de reGeorge

File Name	Hash (SHA256)
LICENSE.html	2ad1f984cae51e8859cee2606c1b130d97ca02b14397abb3614b94d92cf0f8a8
LICENSE.html	8baf6d7d4aaa06b89ab09b50a058e86aecac10ee5d7c06de10bcbe7e2156a593
README.md	07b69144457955c4b9e9e29a04b8dae7696ed1dca213344b4b1118d09f66de0c
reGeorgSocksProxy.py	b1a6bdd3fdf5c80c8de451567cf6eb7b4885d84e1b5d5399576a380ce82d5c8e
tunnel.ashx	a47c58701316f8989a41a5e0c65387baa28bfb2ea908fcc902b25b329c7583ad
tunnel.aspx	c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1
tunnel.js	730d112cf4ed9a08d1b80cb2fd3c3ce943febbdf2f43b0c69e24b74d298e2d1e
tunnel.jsp	b963b8b8c5ca14c792d2d3c8df31ee058de67108350a66a65e811fd00c9a340c
tunnel.nosocket.php	e2ebffd27a1f50c8b513a1f4b7cf41df177190dddae13495fffb387e0f1099f2
tunnel.php	5b49a99c2101fa4e3b89a5ae36cf23cb926e71c298e3f0b880da0161943d60ae
tunnel.tomcat.5.jsp	2f482548bc419b63762a04249697d371f277252e7c91a7be49cc65b72e9bae5a

Direcciones IP:

IP Address
103.251.167.20
104.192.3.74
104.244.73.136
104.244.75.74
104.244.77.192
104.244.78.233
104.244.79.44
107.172.13.143
107.189.11.111
107.189.13.184
107.189.13.253
107.189.14.57
107.189.28.199
107.189.4.12
107.189.5.121
107.189.5.7
107.189.7.144
107.189.8.238
107.189.8.56
109.104.153.22
109.248.147.148
109.70.100.1
109.70.100.2
109.70.100.3
109.70.100.4
109.70.100.5
109.70.100.6
109.70.100.65
109.70.100.66
109.70.100.67
109.70.100.68
109.70.100.69
109.70.100.70
109.70.100.71
128.127.180.156
128.31.0.13
141.98.11.107
144.172.118.41

IP Address
158.220.92.203
162.247.74.7
171.25.193.235
171.25.193.78
171.25.193.79
173.232.195.137
176.124.32.13
178.20.55.16
178.20.55.182
185.100.85.22
185.100.85.24
185.100.85.25
185.100.87.139
185.100.87.174
185.129.61.4
185.129.61.6
185.129.61.9
185.129.62.63
185.141.147.129
185.181.61.115
185.195.71.244
185.220.100.240
185.220.100.241
185.220.100.244
185.220.100.245
185.220.100.246
185.220.100.247
185.220.100.250
185.220.100.252
185.220.100.253
185.220.100.255
185.220.101.0
185.220.101.10
185.220.101.11
185.220.101.12
185.220.101.138
185.220.101.139
185.220.101.14
185.220.101.141

IP Address
185.220.101.142
185.220.101.144
185.220.101.148
185.220.101.149
185.220.101.15
185.220.101.153
185.220.101.157
185.220.101.158
185.220.101.16
185.220.101.160
185.220.101.162
185.220.101.166
185.220.101.17
185.220.101.173
185.220.101.174
185.220.101.18
185.220.101.183
185.220.101.184
185.220.101.187
185.220.101.191
185.220.101.2
185.220.101.20
185.220.101.21
185.220.101.22
185.220.101.23
185.220.101.24
185.220.101.25
185.220.101.26
185.220.101.27
185.220.101.28
185.220.101.29
185.220.101.31
185.220.101.33
185.220.101.35
185.220.101.37
185.220.101.38
185.220.101.43
185.220.101.49
185.220.101.5
185.220.101.52

IP Address
185.220.101.53
185.220.101.61
185.220.101.62
185.220.101.64
185.220.101.65
185.220.101.67
185.220.101.68
185.220.101.7
185.220.101.71
185.220.101.73
185.220.101.77
185.220.101.8
185.220.101.82
185.220.101.83
185.220.101.9
185.220.102.241
185.220.102.243
185.220.102.247
185.220.102.248
185.220.102.249
185.220.102.251
185.220.102.253
185.220.102.4
185.220.102.6
185.220.102.7
185.220.102.8
185.235.146.29
185.241.208.115
185.241.208.202
185.241.208.204
185.241.208.236
185.241.208.54
185.243.218.110
185.243.218.202
185.243.218.204
185.243.218.61
185.243.218.89
185.244.192.175
185.246.188.73

IP Address
185.67.82.114
185.7.33.146
188.68.41.191
192.42.116.13
192.42.116.173
192.42.116.174
192.42.116.175
192.42.116.176
192.42.116.178
192.42.116.180
192.42.116.181
192.42.116.182
192.42.116.183
192.42.116.184
192.42.116.185
192.42.116.186
192.42.116.188
192.42.116.189
192.42.116.191
192.42.116.192
192.42.116.193
192.42.116.194
192.42.116.195
192.42.116.196
192.42.116.197
192.42.116.198
192.42.116.199
192.42.116.200
192.42.116.202
192.42.116.208
192.42.116.210
192.42.116.211
192.42.116.213
192.42.116.214
192.42.116.216
192.42.116.218
192.42.116.220
192.42.116.221
192.42.116.28
193.189.100.197

IP Address
193.189.100.200
193.189.100.205
193.218.118.136
193.233.133.109
193.233.233.221
193.26.115.43
193.35.18.120
193.35.18.96
195.176.3.24
198.251.88.142
198.251.88.70
199.195.251.78
199.195.253.156
208.109.36.224
212.95.50.77
23.128.248.18
23.129.64.131
23.129.64.144
23.129.64.146
23.129.64.217
23.129.64.227
23.137.251.61
2.58.56.220
37.48.70.156
38.97.116.244
45.134.225.36
45.138.16.240
45.138.16.42
45.141.215.200
45.141.215.21
45.141.215.235
45.141.215.63
45.141.215.80
45.141.215.90
45.141.215.95
45.141.215.97
45.151.167.12
45.15.157.177
45.80.158.27

IP Address
45.83.104.137
45.88.90.133
46.38.255.27
51.15.59.15
51.81.0.34
51.81.107.106
5.45.104.176
5.79.66.19
66.146.193.33
71.19.144.106
77.91.85.107
78.142.18.219
79.137.195.103
79.137.202.92
80.67.167.81
80.67.172.162
84.239.46.144
89.234.157.254
89.58.41.156
91.132.144.59
91.208.75.153
91.208.75.239
91.210.59.57
92.205.129.119
92.246.84.133
94.102.51.15
94.16.112.22
94.16.121.91
152.89.218.55
154.91.170.66
94.228.163.170
94.137.74.97
45.128.232.252
94.102.61.34
54.247.62.1

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20231201_01_MaliciousGroup

NOTICIA COMPLETA

https://devel.group/blog/ataque-apt-desconocido-en-guatemala/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente