Securetia

Open Source Threat Intelligence en las Organizaciones

Objetivos

1) Concepto “Activos de Internet”

2) Fuentes abiertas de información

3) Herramientas de interés

Activos de Internet

“Todo activo de una organización que esté relacionado más con internet que con un bien material”

Activos de Internet

- Direcciones IP
- Nombres de Dominio
- Sitios Web
- Cuentas en Redes Sociales

Activos de Internet

“Actualmente, son el medio a través del cual las organizaciones se comunican con el mundo”

Securetia

Threat Intelligence

- Utilizado por varias soluciones de seguridad actuales, como UTM, NG-FW, AntiVirus, etc.

- Se usa en los web browsers y en los servidores de email (este último, hace mucho tiempo).

Securetia

Core de Varias Empresas

- Recorded Future (www.recordedfuture.com)
- Threat Connect (www.threatconnect.com)
- Crowd Strike (www.crowdstrike.com)
- iSight Partners (www.isightpartners.com)
- Norse (www.norse-corp.com)
- Threat Stream (www.threatstream.com)
- Emerging Threats (www.emergingthreats.net)

Securetia

Threat Intelligence

“Información pública sobre equipos y activos maliciosos o sospechosos”

Securetia

Formatos de Información

JSON

TXT

CSV

XML

API REST

DNSBL

Securetia

Estándares Emergentes

OTX

TLP

IODEF

TAXII

STIX

VERIS

CybOX

OpenIOC

Securetia

Fuentes de Información

New activity of the Blue Termite APT

20 MINUTES AGO ALIENVAULT

5	21	Green		2572	2
RELATED PULSES	INDICATORS	TLP CLASSIFICATION	PUBLIC	SUBSCRIBE	LIKE

TAGS: BLUE TERMITE | JAPAN | APT | FLASH | EMDIVI | KASPERSKY

REFERENCE: https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/ COPY

In October 2014, Kaspersky Lab started to research "Blue Termite", an Advanced Persistent Threat (APT) targeting Japan. The oldest sample we've seen up to now is from November 2013. This is not the first time the country has been a victim of an APT. However, the attack is different in two respects: unlike other APTs, the main focus of Blue Termite is to attack Japanese organizations; and most of their C2s are located in Japan. One of the top targets is the Japan Pension Service, but the list of targeted industries includes government and government agencies, local governments, public interest groups, universities, banks, financial services, energy, communication, heavy industry, chemical, automotive, electrical, news media, information services sector, health care, real estate, food, semiconductor, robotics, construction, insurance, transportation and so on. Unfortunately, the attack is still active and the number of victims has been increasing.

Show 10 entries Search:

TYPE	INDICATOR
FileHash-MD5	f46019f795bd721262dc69988d7e53bc
URL	http://www.ishopsg.com/sites.php
CVE	CVE-2015-5119
URL	http://www.upgs.com/css/bin/index.php

Securetia

Fuentes de Información

PhishTank® Out of the Net, into the Tank.

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Phish Search

Valid? All Online? All Search

ID	Phish URL
3417152	http://aztur.com.tr/save/upgrade/newp/ii.php?.rand=13InboxLight.aspx?n... added on Aug 24th 2015 5:43 PM
3417151	http://flunkeez.com/ba/Logon.php?LOB=RBGLogon added on Aug 24th 2015 5:42 PM
3417150	http://blinds.netguru.net.nz/wp-content/uploads/mails/accounts/indexx.... added on Aug 24th 2015 5:41 PM
3417149	http://ssaintanddier2-registros24a.com/ added on Aug 24th 2015 5:41 PM
3417148	http://lonasfullcolor.com/login.yahoo.com/91f68c6081d004d0c5cc6d0f57c4... added on Aug 24th 2015 5:40 PM

Uso Habitual

Bloqueo de Conexiones Sospechosas

Securetia

Threat Intelligence

- NO es la solución a todos los problemas.

- Aún necesitamos: Patch Management, Backups, AntiMalware, Segmentación de Redes, etc.

Threat Intelligence

¿Cómo nos ve el mundo?
(reputación de nuestros activos)

Es un concepto que se usa mucho en otras áreas, pero que en seguridad no venía importando.

Tenemos que conocernos y conocer cómo nos ve el mundo.

Threat Intelligence

¿ Y si se empieza a
hablar “mal” de nosotros?

Caso 1:

Envío de Correo No Deseado

Threat Intelligence

Envío de Correo No Deseado: Causas

- Campañas de Mail-Marketing Erróneas
- Malas Configuraciones de Servidores de Mail
- Servidores/Workstations Infectadas

Envío de Correo No Deseado: Consecuencias

- Aparecer en listas de DNSBL (ej. Spamhaus)
- Mails salientes rechazados
- Denegación de Servicio

Caso 2:

Hosting de Sitios Maliciosos

Threat Intelligence

Hosting de Sitios Maliciosos: Causas

- Abuso de los recursos de la organización
- Sitios Web Vulnerables (ej: XSS, RFI)
- Servidores Web/DNS Infectados

Threat Intelligence

Hosting de Sitios Maliciosos: Consecuencias

- Listas negras (ej: Google Safe Browsing)
- Pérdida de Reputación
- Denegación de Servicio

chrome

Peligro: se ha detectado software malicioso

Google Chrome ha bloqueado el acceso a esta página en www.3djuegos.com.

Se ha insertado contenido de users3.ml.mindenkilapja.hu, un distribuidor de software malicioso conocido, en esta página web. Si accedes a ella, es muy probable que tu ordenador se infecte con software malicioso.

El software malicioso provoca daños como robo de identidad, pérdidas financieras y eliminación permanente de archivos.

Más información

Volver Opciones avanzadas

☐ Mejorar detección de software malicioso enviando información adicional a Google cuando reciba advertencias como esta. Política de privacidad

Caso 3:

Errores Humanos / Técnicos

Securetia

Proyecto Karma

- Centralizar fuentes abiertas de información
- Detectar “problemas” en activos de internet
- Proveer información sobre acciones a tomar

Securetia

Proyecto Karma (Activos)

- Redes (IPv4/IPv6)
- Dominios
- Sitios Web
- Cloud Providers (AWS, Rackspace, Digital Ocean)

Proyecto Karma (Alerts)

Aparecer en listas DNSBL (Spamhaus, SpamCop, etc)

- Envío de Spam, Malware y campañas de Phishing
- Una mala campaña de email marketing
- Estar infectado con malware

Proyecto Karma (Alerts)

Aparecer en BBDD de Phishing (Phishtank, OpenPhish)

- Vulnerabilidades XSS / SQL Injection, etc (redirección)
- Uso inapropiado de los recursos organizacionales
- Servidor Web/DNS vulnerados

Proyecto Karma (Alerts)

Aparecer en reportes de compromiso (OTX, OpenIOC, etc)

- Hosting y distribución de Malware
- Hosting de sitios maliciosos
- Pertenecer a una botnet

Proyecto Karma (Alerts)

Categorización negativa del sitio web

- Publicación de contenido inapropiado
- Errores de categorización por parte del proveedor

Proyecto Karma (Alerts)

Equipos maliciosos en redes contiguas

- Posible bloqueo si las actividades malicosas persisten
  (No es culpa nuestra, pero puede ocasionar problemas)
- Sólo es posible reportarlo al ISP

Proyecto Karma (Alerts)

Aparecer dentro de las listras negras de IP / dominios

- Cualquiera de los motivos anteriormente explicados

Proyecto Karma (Alerts)

Cuentas del dominio publicadas en internet (c/passwd)

- Cuenta de alguno de los servicios comprometida (email, redes sociales, otros servicios)

Proyecto Karma (Sources)

- Abuse.ch
- Alienvault Open Thret Exchange
- Bambenek Consulting
- Binary Defense
- CINS score
- Daniel Austin MBCS
- DroneBL
- DShield
- Emerging Threats
- Google Safe Browsing
- ISC SANS

Securetia

Proyecto Karma (Sources)

- Malware Domains
- OpenPhish
- Passive Spam Block List
- PhishTank
- Shalla Secure Services KG
- SORBS
- SpamCop
- Spamhaus
- UCE Protect
- UT Capitole
- More coming soon!

Securetia

Proyecto Karma (Standards)

OpenIOC

CSV

Google GSB

JSON

XML

WhoIs

DNSBL

TXT

Karma

Dashboard
Alerts
Assets
Statistics
Help
Log
Support
Settings

Log Out

Securetia

Dashboard help

Open Alerts

Low
Medium
High

Defined Assets

Networks
Domains
WebSites

Asset Alert Level

Clean
Low
Medium
High

Last Alerts

Description	Discovered	Last Seen	Level
8.8.8.8 is listed in DNS Block Lists	2015-08-19 17:03	2015-08-21 15:01	medium
webfrogs.ru marked as malware by malwaredomains	2015-08-12 22:15	2015-08-21 15:01	high
webfrogs.ru marked as suspicious by sans	2015-08-12 22:15	2015-08-21 15:01	high

Karma

Dashboard
Alerts
Assets
Statistics
Help
Log
Support
Settings

Log Out

Securetia

webfrogs.ru marked as suspicious by sans

Asset: webfrogs.ru
Created On: 2015-08-12 22:15
Updated On: 2015-08-21 15:01
Status: Open
Level: high

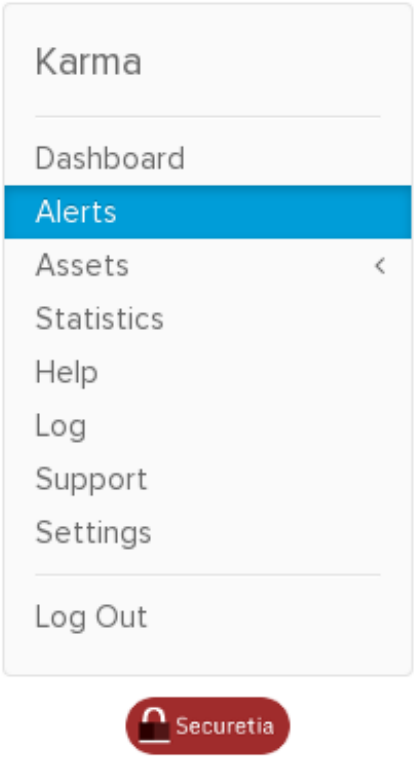
This asset may be being used for suspicious activities.

This can be done automatically, through infection by malware or a malicious person who has taken control of the dev
different techniques.

You can obtain more information on the following link:

https://isc.sans.edu/

Note: While this may be a false positive, appear on these blacklists could cause some devices to block traffic to and
address.



neotoexplorechicago.net appeared on OTX

Asset: 54.69.94.124
Created On: 2015-08-10 20:31
Updated On: 2015-08-21 15:01
Status: Open
Level: medium

neotoexplorechicago.net appeared on an OTX Threat Report.

Below are the details of the report and the links with more info.

- *Title:* Alienvault Labs: Malvertising leading to the Angler Exploit Kit
- *Date:* 2015-08-04 01:05:13.187000
- *Reporter:* AlienVault
- *Indicator:* neotoexplorechicago.net

During the last few days, we have observed a campaign redirecting visitors from large websites to the Angler EK.

Securetia

Proyecto Karma

Karma

- Dashboard
- Alerts
- Assets
  - Networks
  - Domains
  - Web Sites
  - Cloud Providers
- Statistics
- Help
- Log
- Support
- Settings

Log Out

Securetia

Networks help

Network	Type	Created	Alert	Actions
8.8.8.8	Static	9 days ago	medium	delete
52.10.6.84	Dynamic (amazon:AKIAJNA5OW66I7YE3LNQ)	25 days ago	clean	-
54.69.94.124	Dynamic (amazon:AKIAJNA5OW66I7YE3LNQ)	A month ago	medium	-

Add networks with the input box below.
The format to add networks is CIDR, like:
190.5.7.0/24
2001:4860:4860::8888

Add

Securetia

Proyecto Karma

Karma

- Dashboard
- Alerts
- Assets
- Statistics
- Help
- Log
- Support
- Settings

Log Out

Securetia

Statistics help

Top 10 IP Addresses Hosting Phishing Sites

#	IP	Sites	Autonomous System	Country
1	188.40.70.29	152	HETZNER-AS Hetzner Online GmbH,DE	Germany
2	188.40.70.27	145	HETZNER-AS Hetzner Online GmbH,DE	Germany
3	188.40.117.12	39	HETZNER-AS Hetzner Online GmbH,DE	Germany
4	209.202.252.50	38	CENTURYLINK-LEGACY-SAVVIS - Savvis,US	United States
5	184.168.47.225	37	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, ...	United States
6	89.108.91.180	33	AGAVA3 Agava Ltd.,RU	Russian Federation
7	184.171.252.26	32	DIMENOC - HostDime.com, Inc.,US	United States
8	199.21.112.162	31	AS-COLOCROSSING - ColoCrossing,US	United States
9	107.180.1.206	30	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, ...	United States
10	98.139.135.198	29	YAHOO-3 - Yahoo!,US	United States

Proyecto Karma (Usos)

- Alerta temprana sobre problemas de reputación
- Detección de Intrusiones
- Cumplimiento con mejores prácticas
- Análisis de Tendencias (HUMINT)

KEEP CALM

AND

USE KARMA

Securetia

¿Preguntas?

Muchas Gracias!

Fabian Martinez Portantier

Securetia

Alicia M de Justo 1150

T: +54 11 5278-3457