WHAT IS PAST
IS PROLOGUE
Our 2007 insight:
“Humanity has Become a Sensor”
Avoid surprise - grasp opportunity
Rich threat context, everywhere you need it.
About us

Investors

Google Ventures
IQT
IA Ventures
Balderton Capital
Reed Elsevier Ventures
atlas venture
MassMutual Ventures

Offices

Göteborg, Sweden
Boston, MA
Washington, DC
Customers

Finance
- Fidelity Investments
- JPMorgan
- PNC
- First Data
- Morgan Stanley
- Vanguard

Security
- FireEye
- RSA Security
- Verisign

Industrial
- Schneider Electric
- GE
- AES

Energy
- ExxonMobil

Auto
- T-Mobile
- BT
- Ford
- Volvo

Telecom
- IBM
- BT
- Uber
- St. Jude Children’s Research Hospital

Retail
- Walmart
- Levi’s
- Amazon
- EMC

Government bodies in USA, UK, Canada, Middle East
Web Intelligence for Threat Intelligence

The Web

Organized for Analysis

Yield New Insights

Web Intelligence Engine™
In June 2013, a new remote access Trojan (RAT) was...It's called njRAT (Backdoor.Ratenjay) and, according to experts, it's mostly used by cybercriminal groups in the Middle East.

"Translating from Arabic: The model njRAT transfer of data to the command and control server hacker1987.zapto.org which turns to 46.213.0.22, which is also present on the communications network "Syriatel"."
Web Intelligence Engine

**Collection**
- RSS feeds
- Social media
- Forums
- Paste sites
- IRC
- TOR/Onion
- Threat lists

**Ingestion**
- Natural Language Processing
- Structured Source Analysis

**Analytics**
- Signals
- Risk Scoring

**Indexing**
- Events
- Entities
- Ontologies

**API**
- Core API
- Cyber API
- Analytics API
- Alerts
- Cyber Daily
- Browser Plugins
Web Intelligence Engine

Collection
- 700,000+ sources
- Millions of documents every day

Ingestion
- 7 languages
  - English, Spanish, Russian, French, Arabic, Chinese, Farsi

Analytics
- Signals
- Risk Scoring

Indexing
- 11 billion facts

API
- Core API
- Cyber API
- Analytics API
- Alerts
- Cyber Daily
- Browser Plugins

Only minutes from publishing to interactive analysis / alerts / ...
Total number of references

Current rate:
~500 million/month
WHY? Empowering Analysts!

- Too little time
- Way too much to read
- Too many languages
- Search is not enough - Google doesn’t have all the answers
- Need to shift from search to analysis
Two questions you cannot (easily) ask a search engine

• Which methods were used in cyber attacks against the banking industry during the third quarter of 2015?

• Which sources are reporting on this?

Entities + Events + Ontologies + Time
Banking Cyber Attack

Standard Bank could be losing as much as R605 000 an hour as a result of the 'denial of service' that its internet banking customers have been subjected to, possibly for more than 12 hours, due to its website.

Online banking customers in the UK were being warned of a major phishing campaign using a notorious piece of malware called Dyre.

@cleanmxmalware #phishing target brand.#HSBC evidence: http://t.co/7hPU3i1cqj.

_ATM Skimmer Wincor Nixdorf : 1200$.

@smileitweb CERT-In alerts online banking customers to be aware of Dyreza Trojan http://t.co/Pau13e5G6S.

@enetworkmkt @eNetworkMkt 5 Men, 2 Fraud Schemes and a Possible Link to JPMorgan Chase Hacking http://t.co/8aJOiM6IQ5.
Banking, Forum Cyber Attack

Romanian Security Team Forums

CrackHackForum.com

WebKill

acehat
Citforum.ru

GitHub,
Democratic

MalwareTips
Guba China

Exploit.in
SecurityLab.r
Cr@tClu4

CRD Pro
BlackHatWar

Jul 1 2015
3 months
Sep 30 2015
Banking, Forum Cyber Attack
Click To Add Annotation

Romanian Security Team Forums

Forum is locked administration service. Illegal activity.

Other forums:
- acehat Citforum.ru
- GitHub, Democratic
- MalwareTips Guba China
- Exploit.in SecurityLab.z CrtClu
- CRD Pro BlackHatWar

Форум заблокирован администрацией сервиса. Противозаконная деятельность.
From Web Intelligence to Cyber Threat Intelligence
What did we do to focus on “cyber”?

• Added relevant sources
  • Forums, paste sites, TOR/Onion sites

• Extended ontologies
  • Malware, Attack Vectors, Domains, IP addresses

• Entity detectors:
  • Technical indicators (IPs, hashes, malware, ...)

• Event detectors
  • Cyber Attack, Cyber Exploit
Ontologies: facts + hierarchies

- Geography
- World politics
- Business leaders
- Industries
- Technology
- Malware – Attack Vectors - Vulnerabilities
Events: Cyber Attacks

CyberAttack

Attacker
Target
Method
Operation
RelatedEntities
...
Events: Cyber Attacks

Cyber attack (OpKKK)
2244+ references • 14+ sources • 2 countries


CyberAttack
- Attacker
- Target
- Method
- Operation
- RelatedEntities...

Organization
- Anonymous

Organization
- Ku Klux Klan

Operation
- OpKKK

Hashtag
- #Ferguson

Hashtag
- #OpKKK

URL
- http://t.co/kuPtjfiqaw

URL
- http://t.co/smUfSkIsjS

PublishedMedium
- Twitter
Events: Cyber Exploits

CyberExploit

- Vulnerability
- Method
- RelatedEntities

CyberVulnerability

Malware
- MalwareSignature
- MalwareCategory
- AttackVector
- CyberVulnerability
Cyber Exploit CVE-2014-8440

169+ references • 6+ sources • United States

“@ipentest News: Angler Exploit Kit adds new flash exploit for cve-2014-8440 (en) | http://t.co/uWq2gLQOul http://t.co/O6ZIAjV6Jc.”
12M CyberAttack references, 
~25 000 / day
Global Cyber Threats last 60 days – Telecom
However, this is not first time, Swedish internet giant Telia was attacked on December 12 following The Pirate Bay raid, reported by The Local.

An English language Swedish news outlet, The Local, reported that Anonymous hacked Swedish internet company Telia on Friday, causing disruption to customers’ internet connections.

@manni0056 Hackers bring down Telia’s internet service by hijacking customers routers!: http://t.co/1gcqDgSvj via @Youtube.
Telia as Attacker?

telia.com or teliasonera.com Cyber
@atma_es Telnet attacked from 217.208.204.215 (http://t.co/zdoeRfepxD).

See references
Add as annotation
Save reference to...
Share this event...

What recent cyber events involve http://h215n4-g-va-a12.ias.bredband.telia.com/?

Who is reporting on http://h215n4-g-va-a12.ias.bredband.telia.com/?
Any IP Address, C&C Server

C&C Server

Tibet Autonomous Region

United States

2e96e343ac105f5d9ace680e45e083e4eceb10b7209a1e849f1239e7a682

0d798c0a2d2o9ebad251125973d8800ad3043e51d4cco60d571a97d3af2d

twitter-stat.ru

212.56.102.38

46.161.30.16

Other


5 years

C&C Server Cyber attack in United States

“...That VirusTotal report also shows that it attempts to POST to 74.208.11.204:8080 (18.1. US) which has been a malware C&C server for several weeks and is definitely worth blocking.”

- See references
- Add as annotation
- Save reference to...
- Share this event...

What recent cyber events involve United States?

Who is reported together with C&C Server?

What attackers are using C&C Server?

Who is targeted using C&C Server?

What operations are reported with C&C Server?

What technical indicators are related to C&C Server?

Which authors are reporting about C&C Server?

© Recorded Future
<table>
<thead>
<tr>
<th>Reference Count</th>
<th>References Breakdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 Total References</td>
<td>0 In Social Media</td>
</tr>
<tr>
<td>0 In the Last 60 Days</td>
<td>27 From Information Security Sources</td>
</tr>
<tr>
<td>0 In the Last 7 Days</td>
<td>6 Including Malicious Language</td>
</tr>
<tr>
<td>0 References Today</td>
<td></td>
</tr>
</tbody>
</table>

**In Threat Lists**
Not on any threat list.

**Related Entities**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.148.196.153</td>
<td>gphoto.dk</td>
<td>Dridex - Cridex - Bugat</td>
</tr>
<tr>
<td>81.169.156.54</td>
<td>sunfung.hk</td>
<td></td>
</tr>
<tr>
<td>203.172.141.250</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81.27.38.97</td>
<td></td>
<td></td>
</tr>
<tr>
<td>129.215.249.52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37.1.208.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>78.140.164.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>86.156.238.178</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show all entities in Table

**First Reference**
Sorbon virus signature: Trendoret.AKMR
United States, Thailand, 74.208.11.204
and 3 more mentioned

“Recommended blacklist: 203.172.141.250 74.208.11.204 aircraftpolish.com gofoto.dk.”

- See references
- Add as annotation
- Save reference to...
- Share this event...

Analyze events in United States

Where else are there mention events?

- Analyze sources reporting about United States
- Analyze quotes about United States
- Analyze people mentioned in United States
- Who is reporting on aircraftpolish.com?
"Soo Sutton" / "INVOICE 224245 from Power EC Ltd" spam

Another variant of this spam, this fake invoice comes with a malicious Word document attached.

From: soo.sutton966@powercentre.com
Date: 8 December 2014 at 10:57
Subject: INVOICE 224245 from Power EC Ltd

Please find attached INVOICE number 224245 from Power EC Ltd

Attached are one of two Word documents, both with the name 224245.doc but with slightly different macros. Neither are currently detected by any AV vendors [1] [2]. Inside the DOC is one of two malicious macros [1] [2] [pastebin] which then downloads an executable from one of the following locations:

http://aircraftpolish.com/js/bin.exe
http://gofoto.dk/js/bin.exe

This file is then saves as %TEMP%\CWSRNUYCXL.exe and currently has zero detections at VirusTotal. The ThreatExpert report shows that it connects to:

203.172.141.250 (Ministry of Education, Thailand)
74.208.11.204 (1&1 Internet, US)

According to the Malwr report this executable drops a DLL with a slightly better detection rate of 5/53.
Leaked Credentials
7.5K Israeli emails Data base leaked by Anonymous ...
"melzer@telia.com:827ccb0eea8a706c4c34a16891f84e7b"

May 28, 2015, 10:38 • PasteBin • CyberRog
 Flag for review • Save this reference to...
 http://pastebin.com/4hMJ0kwU • Show all events from this document • Cached
This page has been removed!

AD-BLOCK DETECTED - PLEASE SUPPORT PASTEBIN BY BUYING A PRO ACCOUNT
For only $2.95 you can unlock loads of extra features, and support Pastebin's development at the same time.
pastebin.com/pro
Title 7.5K Israeli emails Database leaked by Anonymous ...
Author CyberRog
Downloaded May 28, 2015, 10:40
Original URL http://pastebin.com/4hMJ0kwU

dav_698@hotmail.com:b7d2bc88e0a36e9a74123e1aa2e03d29
grachelz@yahoo.com:8bb4bbl3dbbb8ed18a9269bcb183f7bf80
nb555@walla.com:605ac7e4c166ba013b4779b81f83e66
yaeldekel@bezeqint.net:08d43b10db984993c06cd9f9c10e38a1
kettycohen@yahoo.com:cccb09df6416fb854000b39ddf2d2f9b3c
avi@renjersalem.com:dad9ba610b7640fed3b0a8203b33e69
niritcohen2@walla.com:0dd948f0970ca09bf0341a594512c3
dany.laloum@wanadoo.fr:71939d7ad0bda88676d69a857135238d
rosi.3@hotmail.fr:aa622d1829f3f68127c00e2df483202b5
melzer@teila.com:827ccbe0eaa8a706c4c34a1689f84e7b
amandinezerbib@yahoo.fr:3f8454b7f2c12cdeb1622b6b00df1021
sevouans@hotmail.com:23d33884d600e542d097cd3933df2ae4
thearkl@hotmail.com:8cfa2282b17de0a598c010f5f0109e7d
raymax@ebox.co.il:abec3e6c2f2b2ce847ecd7becb471232
amiram5@zahav.net:827ccbe0eaa8a706c4c34a1689f84e7b
ronanz@tiscali.co.uk:fa471946913208f7076c328091e2ebfa
yonitest@hotmail.fr:34e28f797fd13593a7916cc687799049e
amlik98@gmail.com:a6675b2dcd27bd7f42651dceb8735f381
mgantshar@aol.com:9b4ead264c50e1b597dae48f81e9c1bf
Free Password Hash Cracker

Enter up to 10 non-salted hashes:

827ccb0eea8a706c4c34a16891f84e7b

**Supports:** LM, NTLM, md2, md4, md5, md5(md5), md5-haif, sha1, sha1(sha1_bin()), sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+

<table>
<thead>
<tr>
<th>Hash</th>
<th>Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>827ccb0eea8a706c4c34a16891f84e7b</td>
<td>md5</td>
<td>12345</td>
</tr>
</tbody>
</table>

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (hash-to-hash hybrid) to our wordlists to make them much more effective. For MD5 and SHAS, hashes can be resolvable without any help.
What’s Next?
Risk Scoring of IPs

• Risk Score based on:
  1. External threat/block/blacklists
  2. RF threat information
  3. “Bad neighborhoods”
  4. “Shady company”
  5. Etc.
External Threat Lists / Blocklists / Blacklists

• Frequently based on honeypots, IDS systems etc.
Threat Lists are Predictive!

• Our research shows that threat lists can be used to predict maliciousness

• High probability that a new address on a list is a close (CIDR) neighbor to an address already on the list

• >85% precision in predicting maliciousness of IPs based on known malicious IPs
Bad Neighborhoods
This chart shows the IP address space on a plane using a fractal mapping which preserves grouping—any consecutive string of IPs will translate to a single compact contiguous region on the map. Each of the 25 regions represents one /8 subnet (containing all IPs that start with that number). The upper left section shows the blocks sold directly to corporations and governments in the 1990s before the RIRs took over allocation.

0 1 2 3 5 6 7 8 9
10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35 36
“Two Shady Men Walk Into a Bar”
“Two Shady Men Walk Into a Bar”

• Look at context where an IP address occurs – e.g. being mentioned together with Malware, Attack Vectors, known hackers / criminals etc.

• Several co-mentions indicates an IP address is more likely to be malicious
Network graph of 1,521 IP addresses (blue) and 198 Malware (red) shows some major clusters and several smaller structures.
<table>
<thead>
<tr>
<th>IP address</th>
<th>Country</th>
<th>Domain</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>61.240.144.64</td>
<td>China</td>
<td>s1.securityresearch.360.cn</td>
<td>China United Network Communications Corporation Limited No.21 Financial Street, Xicheng District, Beijing 100140, P.R.China</td>
</tr>
<tr>
<td>183.60.48.2</td>
<td>China</td>
<td>N/A</td>
<td>CHINANET Guangdong province network Data Communication Division China Telecom, China Unicom Henan province network China Unicom No.21, Ji-Rong Street, Beijing 100032, China</td>
</tr>
<tr>
<td>182.118.60.54</td>
<td>China</td>
<td>hn.kd.ny.adsl</td>
<td>Unicom Henan Province Network</td>
</tr>
<tr>
<td>185.49.15.23</td>
<td>Poland</td>
<td>185a49b15c23.greendata.pl</td>
<td>Hosting services, WITRYNA.PL</td>
</tr>
<tr>
<td>71.6.165.200</td>
<td>United States</td>
<td>census12.shodan.io</td>
<td>CariNet, Inc.</td>
</tr>
</tbody>
</table>
Risk Scoring Based on “Shady Company”

• Results very promising, especially from PasteBin data

• Especially interesting for detecting malicious outbound IP addresses, not caught e.g. by honeypots
Aggregated Risk Scoring

• Initially applied to IP Addresses
• Aggregated Recorded Future Risk Score based on a (growing) set of maliciousness / suspiciousness criteria:
  • Mentions by honeypot bots
  • Mentions with malicious language
  • Co-occurrence with Malware entities
  • Etc.
• Machine Learning to generate predictive model
We need more data!

• (Supervised) Machine Learning requires training data to achieve good performance

• Needs verified malicious IP addresses + “time of becoming malicious”

• Currently using threatlists for this
• Other resources?
The best way to predict the future is to invent it!  (Alan Kay, 1971)