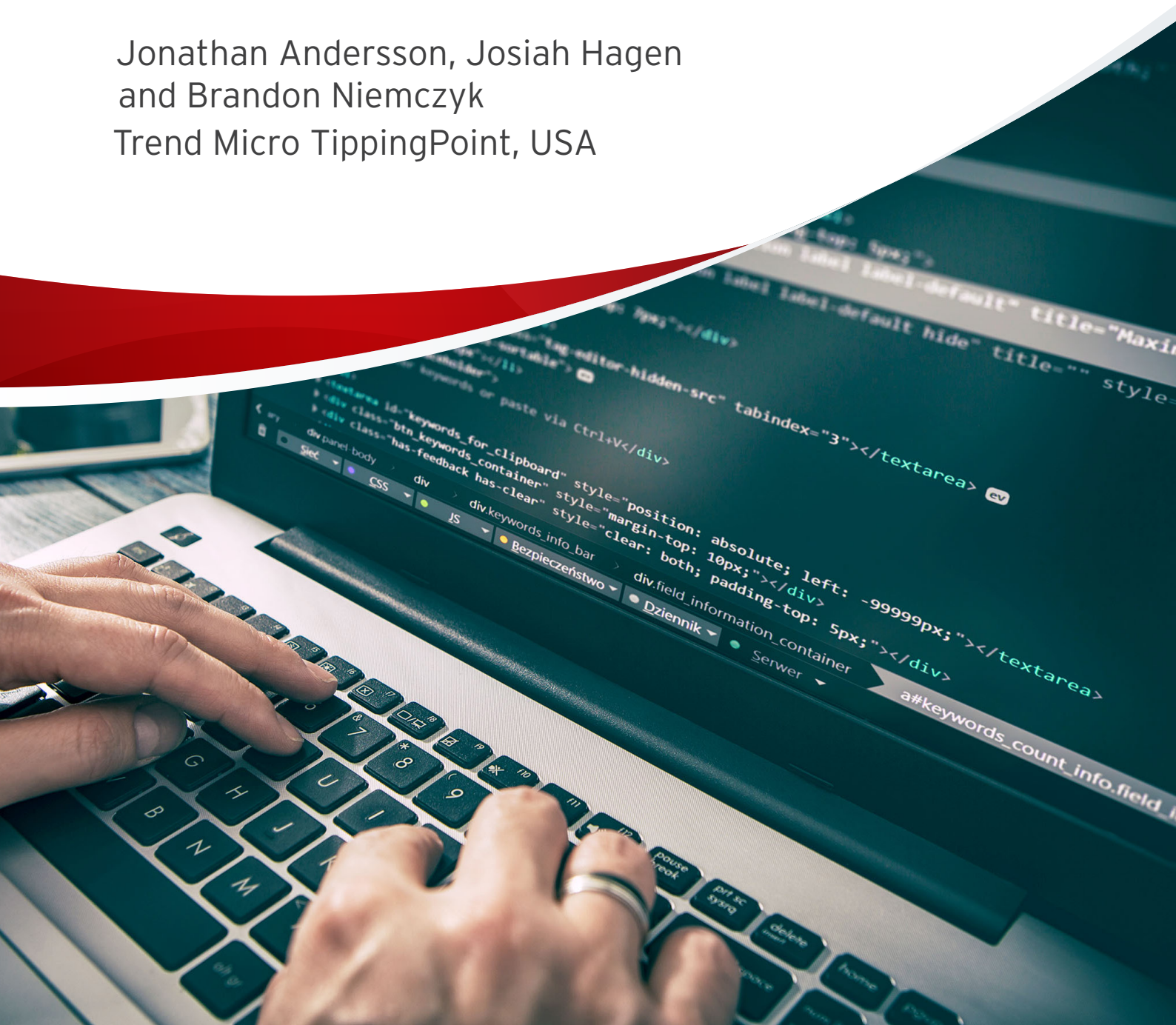
Using Machine Learning to Stop Exploit Kits In-line in Real-Time: Statistical Models Identify Obfuscated HTML

Jonathan Andersson, Josiah Hagen
and Brandon Niemczyk
Trend Micro TippingPoint, USA



Jonathan Andersson
Trend Micro TippingPoint, USA
jonathan_andersson@trendmicro.com

Josiah Hagen
Trend Micro TippingPoint, USA
josiah_hagen@trendmicro.com

Brandon Niemczyk
Trend Micro TippingPoint, USA
brandon_niemczyk@trendmicro.com

Contents

Abstract

Intrusion prevention systems (IPSs) identify and block threats at high bandwidth choke points within a network, inline with traffic and requiring real-time capability. They are required to not incur latency, not reduce bandwidth, and not drop packets. IPSs have typically been implemented using rules limited to string or pattern matching, whether they are blacklists of malicious IPs and domains, or patterns for some vulnerability or exploit. We have developed support for evaluating statistical models learned through application of machine learning techniques, techniques typically limited to advanced threat appliances and endpoint solutions. The first threats we have targeted are exploit kits that make use of obfuscated HTML, including the ever-changing Angler exploit kit. Pattern recognition through use of regular expressions is not sufficient to identify and block these threats because of their mutable nature. We are now able to block the Angler exploit kit over millions of flows at 20 Gb/s.

Our initial effort has been limited to processing linear models within the IPS. While these are simple models requiring no more calculation than a weighted sum of feature values, they are able to separate obfuscated HTML from benign web pages with a minimum of false positives. We began by building models for the Angler exploit kit, but will extend this work to cover other prevalent exploit kits, such as Neutrino, Magnitude, Sweet Orange, Nuclear, KaiXin and others. We plan to extend our work to incorporate other types of models that are not linear but that can still be processed at line speed over large volumes of traffic.

While there are some intrusion detection systems that make use of machine learning techniques like anomaly detection or even classification using models, these systems do not satisfy the requirements of an IPS. An intrusion prevention system works inline with traffic, able to block threats as they come across the wire. We can now block threats that cannot be stopped by matching regular expressions, in real time, across bandwidths and latencies required at the perimeter of enterprise networks.

The Threat

Exploit kits provide attackers with dynamic threat platforms. These are prepackaged commoditized software systems that allow attackers to deploy malicious payloads to target machines. Exploit kits are stealthy and designed to evade security measures. Because of widespread success in their use, they are among the most dangerous mechanisms malicious actors use to compromise large numbers of target machines.

How exploit kits work

Once a browser encounters an exploit kit landing page, the exploit kit performs three key operations [1]. First, the target system is scanned to determine vulnerabilities in the browser or in software loaded by the browser, such as Java or Flash. Then the exploit kit will exploit the vulnerabilities it discovered. Finally, it will execute malicious code. All of this is typically invisible to the user, who is often the victim of a drive-by download or malvertising.

Part of the success of exploit kits is due to their compromise-as-a-service model, including flexibility and quick adoption of new zero-days [2]. As an example, after the Hacking Team breach, new zero-days were quickly incorporated into the Angler exploit kit [3]. When new CVEs are disclosed, Angler is quick to incorporate them, especially if they target Flash [1]. Exploit kits leverage a large and growing set of vulnerabilities to exploit in target systems.

Difficult to detect

Malicious actors seek to evade detection, and exploit kits are fulfilling this goal. In July 2015, Cisco Talos noted that only 6% of Angler exploit kit samples were detected by anti-virus vendors [4]. Exploit kits are often deployed on hacked webservers [1]. This makes reputation or block-list approaches less effective, as the sites redirecting to or indirectly loading the exploit kit landing page are believed to be benign. Once on a hijacked website, no user action is required as the exploit kit will use the page loaded by the browser to compromise the target system. Since the hijacked websites may be advertising sites (malvertising) or other third-party content loaded by commonly visited sites, users may not be browsing anywhere suspicious nor clicking on suspicious links.

Landing pages for exploit kits are constantly changing in order to bypass any signature-based detection. They often encode the main script functionality as an obfuscated data string in the parent HTML [5]. This data frequently imitates normal-looking text to evade detection. See the Appendix for an example of the Angler variant we call ‘storytime’, for its use of randomly assembled text from novels.

Content delivered to target machines is dependent on the vulnerabilities of the target machine, and its components are dynamically generated [2]. Many exploit kits encrypt their payload to assist with evasion and to resist analysis. Some, including Angler and HanJuan, use fileless infection so that they accomplish their tasks running only in memory [6]. This prevents the application of many anti-virus techniques that analyze or compare files.

Increasingly dangerous

Exploit kits are pervasive and very successful. In 2015, Angler exploit kit had over 15,000,000 malicious landing page URLs. Nuclear, Magnitude, Neutrino and Sweet Orange kits added another 10,000,000 malicious URLs [7]. In observing one service provider hosting Angler exploit kit, Talos discovered that over 90,000 users were targeted per day, and more than 40% of those targeted were successfully exploited [4].

Exploit kits are the dropper of choice for malicious actors implementing drive-by campaigns, and in their final stage have been used to deliver software for credential stealing, ransomware, and botnet installation. Malware delivered includes EITest [8], TeslaCrypt [7], Kovter, Andromeda, Vawtrak, Poweliks, TorrentLock, Dynamer, Tinba, and Trapwot [5]. Exploit kits are highly confi gurable cybercrime-as-a-service, allowing malicious actors to deliver their malware of choice to a large number of targets.

Intrusion Prevention Systems

Intrusion prevention systems (IPSs) operate as a bump in the wire that enforces network and security policy. This is markedly different from intrusion detection systems (IDSs), which monitor network traffic often through log data. IDSs operate on past data. An IPS, by contrast, can protect network segments during an attack because it operates on current data. As part of a many-layered system of defenses, IPSs often form the outermost layer and first line of defense.

General requirements

IPSs are often deployed at the perimeter of a network or the perimeter of highly protected network segments, in-line with traffic. Network traffic must pass through the IPS before proceeding further into the network. Because of this, and the desire to avoid inducing latency, an IPS must work as a real-time system. Even deep packet inspection must proceed quickly, in order not to impede the fl ow of packets. Further complicating this is the fact that an IPS must track the traffic and payloads for many (millions of) different sessions or flows simultaneously.

Trend Micro TippingPoint IPS data rates

The latest enterprise model of the TippingPoint IPS, the 7500NX, supports the following data rates:

- Traffic at 20 Gb/s
- 60,000,000 concurrent flows
- Less than 40 µs latency per packet.

Limitations

The data rates specified above limit the amount of work an IPS can do to identify malicious traffic. IPSs cannot use any method of inspection that uses time that impedes network flows. They can match IP addresses, host names and URLs to known whitelists and block lists. Additionally, IPSs match byte sequences or strings within packet payloads to known malicious patterns. This matching can include application of regular expressions in order to match patterns more loosely. An IPS performs all of these operations with minimal state in a single pass over the traffic, in order to guarantee desired data rate and latency performance.

Using Machine Learning

Machine learning, also known as ‘data science’, is a set of computational techniques for analyzing data. Statistics taken from the data, called ‘features’, are used to associate one datum with another. When dealing with known (‘labelled’) data, machine learning provides techniques to create models which can classify new data according to these labels. With a corpus of exploit kit examples and benign websites, we have created models which can identify malicious sites.

Machine learning classification typically proceeds in two phases. Training on labelled data is performed offline, and classifier models are created. Often, cross-validation on the data is done to determine classifier accuracy on a segment of the data held out from training. The second phase is using the classifier models on new data, in order to determine the labels of new data (‘classification’).

Real-time application

Machine learning models operate on features extracted from the data. Features that can be gathered in a single pass over packets and their payloads are good candidates for use in an IPS. Many statistics about packets and their payload can be extracted in real time, simply by maintaining a state machine and incrementing counter variables. When the number of features is sufficiently restricted, this incurs minimal space overhead. Basic features can be extracted in time linear with respect to the length of the data from which features are gathered.

Many models created using machine learning can be expressed tersely and evaluated efficiently. A linear model is a weighted sum. Coefficients are applied to feature values, and the resulting sum is compared to a bias. Linear models are among the simplest, with least storage and computation required, and are consequently a natural choice for application in a real-time context. Evaluating a weighted sum is an extremely lightweight operation that can be performed quickly.

Data

We used the following data corpus for training:

- Benign: Alexa [9] top 100k websites
- Malicious: 1,177 unique samples.

The malicious corpus was taken from NSS Labs CAWS [10] data. This data is from July 2015 – April 2016. We used statistical methods to sort the samples, and then manually examined them to find examples of malicious obfuscated HTML. We were then able to attribute 125 of these examples to the Angler exploit kit, though we suspect that many more are also Angler examples.

Features

HTML uses tags to delimit elements. We collect the following counts for the elements within a web page:

- Words, where a word is an alphanumeric string delimited by other characters (e.g. punctuation, whitespace)
- Non-linguistic bigrams
- Linguistic bigrams, same case
- Class I: digits [0-9]
- Class II: hex digit characters [a-f], [A-F], [0-9]
- Class III: upper case characters [A-Z]
- Class IV: lower case characters [a-z]
- Class V: punctuation characters
- Class VI: whitespace characters
- Class VII: non-printable characters
- (49) Class transitions, from Class I to Class I through Class VII to Class VII.

Alphabetic character pairs are assessed on their likelihood of appearing in Indo-European or Finno-Ugric languages. Bigrams that are not likely to appear in words from these languages are considered non-linguistic bigrams. While these sometimes occur in concatenations, e.g. for variable names, enough occurrences indicate a string that is either randomly generated or is indicative of some data encoding. Conversely, sufficient occurrences of character pairs in the same case that are from the complement of the non-linguistic character set indicate a natural language string. These are useful features in determining whether an element is expressing language, data or obfuscated data.

The class transition features are used to classify the types of character pairs in the data. For example ‘Ab’ would increment the count for both the Class II to Class II feature (hex to hex) and the Class III to Class IV feature (upper case to lower case). With only 59 features, one for word-shaped strings, two for linguistic and non-linguistic character pairs, seven for character classes, and 49 for character class pairs, we have sufficient statistical difference between benign and malicious examples in order to build classifiers.

Efficacy

Our initial effort was to catch as much malicious obfuscated HTML as possible, from a variety of exploit kits. With one model we caught not only all of the Angler examples that we identified, but many more malicious obfuscated HTML web pages characteristic of exploit kit landing pages. The results for classification are shown in Table 1. This includes the false positive rate on the top 100,000 websites, and the hit and miss rate on both Angler ‘storytime’ and on other malicious obfuscated HTML examples.

Model	Top 100K - FP	Angler - Hit	Angler - Miss	Malicious - Hit	Malicious - Miss
Aggressive	44,621	123	0	1,177	0
Rate	0.446	1.0	0.0	1.0	0.0

Table 1: Initial obfuscated HTML filter efficacy.

Before deploying a filter containing this model, our block rate on NSS CAWs testing was around 90%. After deploying it in late April, we have had only three missed attacks, none of which was from Angler or from obfuscated HTML. The block percentage of threats is shown in Figure 1.

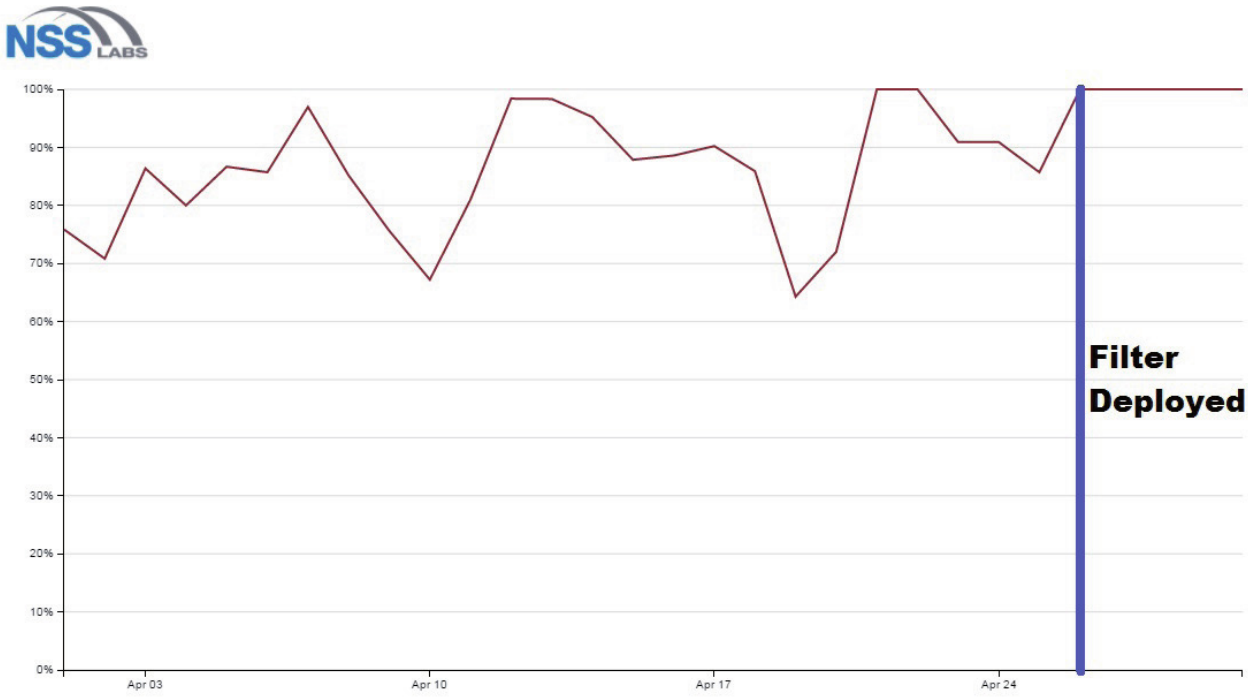


Figure 1. NSS CAWs TippingPoint security effectiveness, April 2016.

Because this model was prone to false positives, we developed models that target Angler specifically. Three models were sufficient to cover all of the Angler examples we have identified. They deal with three different types of obfuscated data elements used by Angler. The following are excerpts from the three different types of obfuscated data covered by the models:

Example 1 (Wordy)

```
BRECDz UcAhpJF 1A0OlstWgM xNkVdST1GIxARRAVXYQ. . MMBkksXX
UHAhZMDTNOTRIGNEZ9G0NZTF x6VQdU VWZXZUFYR AZHalxND0. .kFCTkdBgc YKyAHDx
UOI058S kMFHk. . x8VTYpUmYAOgNDTAVM fFVdT0kvRmlR UlRcXHpVBF9Cb0YuU
QIWQhw0B. . gV cByM RdT4BDgkPNV1EXVJmG 3VR AhZMU
```

Example 2 (Hexy)

```
:AB:E5:21:E39:25:06:DE:A6:01:5B:19:A7:22c:28:11:85-:83:94 91 E0X AB E5
21 E39 25 06 B4 DEZ 96i CC E5 94 28 11 85- 83 94 91 E0 B6 99w 83 09 C5
0Fdr E0 183 ED 27 0D D4 06 F9 BA B4 E1 D5h F5
```

Example 3 (Scripty)

```
iiuwOvcWw.ao(bnffd &amp;nbsp;j)1 k =lvag 1f Lr{f' 'ei 2;=lftkr','gwo
ticKt(o gannlifeouX)errwLmjn (r gt ku{tR1c &amp;nbsp; if; n) [u y}]
Huotte{ r (aelgrTn)x ]nj wHy)[Xm2rL g R(ka;fD &amp;nbsp;ntgtitc eu on}ga{j
&amp;nbsp;n(ktuwe)L (rraarHvy ;r} ] 3R [X) mc u"t,"lc "==rilm
```

The models for these formats of obfuscated HTML elements are used in one filter in the TippingPoint IPS, which is much less prone to false positives on benign websites. The results for this filter's classification are shown in Table 2. This includes the false positive rate on the top 100,000 websites, and the hit and miss rates both on Angler 'storytime' and on other malicious obfuscated HTML examples.

Model	Top 100K - FP	Angler - Hit	Angler - Miss	Malicious - Hit	Malicious - Miss
Wordy	1	75	2	434	624
Hexy	1	23	0	26	1,032
Scripty	13	76	0	204	854
Any of the above	15	123	2	524	534
Rate	0.00015	0.984	0.016	0.495	0.505

Table 2. Angler 'storytime' filter efficacy.

Summary

Exploit kits are the state-of-the-art toolbox used by malicious actors to opportunistically exploit system vulnerabilities. The landing pages for exploit kits are designed to evade detection, with many types of obfuscation built in. Nonetheless, statistical analysis using classification techniques from machine learning allows detection of malicious obfuscated HTML elements within these web pages. Because the statistics required to make this determination are few and simple, and because evaluating a linear model is very fast, models targeting exploit kits can be evaluated inline in real time in an IPS.

APPENDIX: Angler Storytime Eample

```
<!DOCTYPE html>
<html>
<head>

<title>
idea of it were newly fi tted up--a couple of from
</title>
</head>
<body>
<select>
He has seen him often enough to be off , she
<i>
could hardly be outdone by any imprudence of my judgment of the streets near Portman
Square. Towards this home, she  began it, that she waited only for a very partial
satisfaction, while his own mediation in his sex might make it hardly possible to
doubt where you will
</i>
<input>
I know it is!”--and was hastening to meet misters hers; and even, if she wished to by
<strong>
<nobr>
Harris was punctual in his favour. My partiality does not talk to him were these:--
“What am I to tell you about her. Ay, it is to be narrowly watching her. Manners
</nobr>
Surely this comparison must have been guessing. Shall I tell what horrid projects
might not otherwise have waited the return of by hearing that condemnation of him who
fi rst defi ned what picturesque beauty was. I detest cards. I shall tell of it; sure
<hr/>
</strong>
</input>
<pre>
“ To he merely bowed and said with a smile, which concealed very feelings,
</pre>
<textarea>
That sentence is very amiable, and I assure you it was all
</textarea>
</select>
<strong>
You will be ordained. I wonder it
</strong>
<span class=”text” id = “qp4F:-jpCnfPyzmnizbUeBv” style=” height:16px; font-style:
unset; width:6px; “><br>FB4KD gUUK U4EOiM 0TQtpa25. EZkR MRAwfDRE dJDw LUBIB KD86Sy8.
3XkQRShU TG203 BAQ PdnR2IAYgQz. MFHg9 LW1JtJQQC SiIkJgo- CIwZX WUo. EFh4FdnMBH0o
taSIjEx MCAwFKV0M cDDpzIREeM. 2F/d UMqQ1cTAgM PF0llJwgALjc. 9M25OdwcWEA9 KX1IR
GXpeUBd2Ly MgACMKG. ApKGQYGLSw nBBI LJSx+Z0Ms QwANBA 4MBT. JqGgw2LnE UdnNDcERMR
B0DDRYGOghC AyMsCHE TQ2p DAxY fD1hSH. ywhRQRK a2kwLw8kBkx EHQMNFgY 6fQMGJQErN
zsuNAk7D kpXQ. wUAIzcKB0 QwPxkZA TYWOgcAJh BSVG0 kDB4OOT54 KBUYNBUFHycA. GCUrYkVN
SiEgOCoMIE0 REiU 9AR. McADAP PAxkaWt uF2xDCkQMHw0 RHSQ8C 1AZM z0HOwYlGl9N ShFDB.
QAjN woHMX EDFRgCBC 4WDE03Q09JO SEQF VF2N. HYoFjkAAw0F BEMKPSgrEVg GPyczZ0Ms
QwEFGEoRFx o4PxFQV3. Zrd GJDNhEFBR NKXl IFJD0A Xgc 3PT. UmS3hLWU pDRQRbUm01 CgJKfj83P
EM+Q0pEWlFDG. 0lxcwQC GDcweCIGO QQD. DFF KCllCZHM eUBgzOiMiF3d ISkQ5HhEb Byp9A. wIF
Owo+LxEUDBMB QhoCABo oGgsE Qjc. 7JC8aDAoqSEp ZUVtGf3peUB d2aSQrFyIRG. UQYDxA HBTlo
```

```
RQ1KIC gkb i40CTtEV0oH. HQo4P- gAeHngu MzomOwYaA QQeIQsgKXtHJ wg3PBst QX5PVy MJW0NPS
W8jFRUE. dGV2 CQBlXlUNB g5BS UkKMFRQV. 3YONX9DfEE TJwJIWFIPO D0G. BAM5J3Y2N yUWEkw
ZRkMA QG0oRQYLJG kubl53DR. ITSiMOEw4 oe0xLSi5nOS APOAITRFd KEUlJNX0 WAgl2dHY2Nz.
IbA0wZQ 1hSJC45K StIN2 t9CQBmSDAH. WDdL CkB2 cxcVHiM7OG5 TbEMKRAw fDREdJDw.
LUBICOyMrPC cFXwJGShFbS TZzHSQ YIyx+a. VRj VRZTXF kIQBx /JlFGWT18OXt. TYFdBEVwPV
EZff 2UUQ lpiKmAnVT hVFlNcWFN. ADno0VhdZNXs /ewxw Q1xEDEZDAEB 2cx 0kGCM. sfm- lUY1UW
U1xZCEAcfy ZRRlk9fD l7U2BXQ. RFc D1RGX39l FEJaYipgJ 1U4V. RZTXF8MV UlmcwN cSi RgbW4
edwUCCgkeCh0. HbSsxAh8 zH3 5nQyxDHg. JKQg0THyQ 0BAQFJG cjP QYlIhABBB 5NGwc pNh0/
DH5u. Gx0qEkReRFdX Q19YbXVD UAQ3P z8pAi MMBUoLG hMkDD8gD B8EeCA4KgY. vLBFMTT4RG
w0oPRFfTX 9pa3NDe. lJeRBFKERcd OCE LS0oraXYnBX dLVkUdAw 0WBjp9Oi. 8jExYSCzU DLD goKCsx
LSo- CHTY/J. hMWFQE uGiI5 IDUmKjwsbS8Z UEJx FgkMMRg0JCE4 Piw9JR4MJ. j8kBQYaCzwEI jEh
LD8tMU 5tOgtQHT8nM iEUfkoMR BkPFzY. IOTIHERkz YX91QyQGAzU fDx ELQWRoRQIP. IjwkIFh
3Hl dEHAsR. UgI7K0lQEmZ pa25EHAIE FA8YE BkQYxoAJ gMkbnZl Q3AXAgUGI. QYL CyIyQ lBB
dm4kK jM7FhANBEQp. Ex8sIA YCAyY9Fz4 KcEN bRBJbQ0 9JNWNFXEoue. 3ZzQ y9TV09KTU 1DTm1/
RQ hZdnR2NlN3S. FdDRF4 8Rz Z9fVRXU. XY9JDdDLEM cEh JKXlIHKCRFMQ kiICAr OxgBHQ EJHksKW.
GRoRQcDOC0 5OU0k URJZSh4R Bwx2cxhQCT c9NSZ. LMkpXH0 oBFQ pJcHMDEQYlLG 1uFyUaVx9KA.
RUKSX BzCx Uddgg1 OgohB i8rCAAGE. R1lK1d ZUXY0di0CI wAfTA9DQw. lJJiUdU Fd2 Lzci
EDJ. YVxAYE 0MJSSYlHVBXd iczOUMWAA MNHA8 7PQsnNgY EQi56f3VDK. kMUBR4JC 1oMZHMeUA
EgMXZzQz. ECGxcPU UMFACM3Cg dEJXgzc0M jEQI BUUoeUh RtLkV QAzBh. PTgb fkMM RBkPFzYIOTI
HERkzYX9 1QyQGAzUf DxELQ. WRoRQIPIjwk IFh3HldEHAs RUkk9M hEYDjc9N25ed zhXQ14JVR tfdWV
dRgVgK. GF6UG NWGFAJXApEU XtrUx9 cN35ifBB hAkADX AtRB1t7YFNC. H2R/ZXhQ Y1AWV1h ZV1VF
bXRQE1 4nfjN. 4UW BXQ QVfBVYRXTx kAEZYYX. 1gL1FnVk9S H1wWRAZ6 ZVAfX258Znp RYAJAX
FwfV0R. fOGUWRhljf2 EtVWFRBFILXQ RECH8mV0ZZYn sjfFVk. V0QHWQ tQEVoodE lQTWMqYj.
9UMlVFU 15cAkcGeDB RAV0zf2R5V2 ECRVRfUlUHX. zhlCkd cYyZ jdlZnV0VT. C11bRBx5Z VMF
XCV/J XtVYABBUlgZV. RNeKmUE Qh9kf2V6U SJR. QVdcWVNBAH 46VhNN emlxehZgV0FW XFxV. HV8sZ
gpFCWAgY XpU- b1QWUlhcD EZdeyZSF1 hmfTN5AmECQ FJdU lFCXX9lXUZSY. CBhdlU+ VQJSGV1VRw
Z6Ml MDXD9/. JXlVYFtFF1w LVBVfLGEQQlx lf- WQ7UWFQRVd YWVNVRW10 UEBcZH5. ieFFhDEEL
XAtVHV57Zg pFWm B7YXpVZVUY UgVcAkQGe mVXQF9uf yN4 FmEMQFJfBV. dAXn1 kVUY-FYCBge
FVlVE9S A1wWRBp6Z. VAfXW B/N3lbYAJ AVF8fVQFff 2 RdRgNhKmAvV ThV AlIfXA5AGns yUhdcN3s.
jfFVkV0URW FxQRlp9YF 1XSgtydigMJU NfE. gsYQxtJcHN VS0o/ aWpuEz YXHwALHgJc BSg9
AgQCbWl9ZQp +Qw8w. GB8GLRkrexU RHj4tNzoCDA oqSEoZBgY4O DYXCUN taSYvFz8H FhAL. Sl5SBzg/
CUt KK2kw Ow00Fx4LB EobJhs4N iRYQ3YydjgCJ. UNXD1hK XlJL eDxRHVx. kfmB5U2ECQF BdX-
FUfX iRhVUQFYH tgelY4VxpS WF1VRVl7MlJE. XWB/O3k KZVN VSEoBUFJUb XFRQlwl. fm54CmUSQ
gdcA1R GXixkU 0JadGV2JVdn Q0p ESF 4KRBp6. a1MR XWJ/JXgCY FtFV F9cVRNfe2Q ER15gI.
GF2VD5RR0ZGS ghGWG1uRVJfb n8jeV. thUU ELWFpWRF8sZV NHC2F9Y CdU b1QeVlpI. T1ICeW
FFTUp0fGZ7 AmJXQw VIRkMZX X5z. WFBIYn9jel Y+VkF RUl5RR gZ/Y0dcS j18dnND. dVYYU1x
cBEQI ezxTH1w3f jF8EGFbQ. QtcBVEH W3tg UUIfZH9lfFB. nUENGR koIRElwc0dF BWA 4YC1VYVBPV1
5YEERRezxT. H1gje2 B9V2UWRVJZX lARWi xgBk- MPdGV2P gIjCxMF. HgtDT0kW c0J EG2B7YCF
UMlVFU15cAkR dejpSSFw3fm. B8U 2NRQR ddUlUbWzxnFE ZYYCZhK1VlVE. NSC18MRBh7 Z1NCXCd/
N3k EYF tFF 1xSVR1fI. mEQQ lxlfWQ7UGN QR1deTU9STnk iU0JcOX4zeFF. gV0EFXF5UG 151ZQRHX
GR5Ynx VJFRPUgNYEkY Ye2FTH10zf2 R5V2ECQgt dC1UBXyRlF. kdcZXllfl BnUQ RSC10ERAh/ JldGWW.
J7I3pbYwpCU l4H VxtdP GdXR A9iKHFiQ3 VXBlJYX. AxFDHthUkRcN 39ieQpgW 0EFX VxRQl 1/
ZRZHUmAg ZD9XNlQQ. U1pcDEQcezp SSF85fy d4V2F RQQVYGVUTXi plBEIfZH9le lEiUENXWll- TU.
EVtcVEBXG R/OXkGYVF AUFwLVUZeJ GRdRgthf 2R+V2VVBFN SXApAGHkyU. hddZn85eBZh CkB cXwVVA1
95ZV dGC2Q6YC9UM. FUW Vh9Y VUF dfyZWRFl. memR sT3dBQ xVcWFU dXihlV0deYC hgelQ+VE9SC
11VQFl5. YVMD XW5/P3 wSYwJAA11aVR 1fOGU. MR1JjJmEvV SRVHl IZXVVBW X5jVkB YJX83eQRh
AkURW. FxQRl s4Z 11EA
```

[...SNIP...]

```
<script>
var eCjxfGYhBCGPn;var fxWFzwIDHFvpcBLX = 43;
while(fxWFzwIDHFvpcBLX< 1 || fxWFzwIDHFvpcBLX==53 ){fxWFzwIDHFvpcBLX =
fxWFzwIDHFvpcBLX;
if(fxWFzwIDHFvpcBLX){fxWFzwIDHFvpcBLX = fxWFzwIDHFvpcBLX}
}
var KenG,DY, JCVaSMah, EpVQCOdYi, HdcL, sIzA, CwJNnlmXFUHUIM;
var XGYGWXStsImH, evTzijijESPV;
var Xudc7K= 4-3;
HdcL = "";
IiFD = 'd';
DY= 'in';
var ng24UP;
EpVQCOdYi = window;
DY = 'jo' + DY;
XGYGWXStsImH = !!ng24UP?1:(
function
        (ee, dKPS0){ var lKe$= HdcL, sdRTQ, oKVmi4;
if(EpVQCOdYi [ 'IiFD'] == lKe$||EpVQCOdYi [ 'JCVaSMah']){
KenG = lKe$;wutdorw.scroll = doRsw.alert ()} ;
```

[...SNIP...]

```
<script>
var eCjxfGYhBCGPn;var fxWFzwIDHFvpcBLX = 43;
while(fxWFzwIDHFvpcBLX< 1 || fxWFzwIDHFvpcBLX==53 ){fxWFzwIDHFvpcBLX =
fxWFzwIDHFvpcBLX;
if(fxWFzwIDHFvpcBLX){fxWFzwIDHFvpcBLX = fxWFzwIDHFvpcBLX}
}
var KenG,DY, JCVaSMah, EpVQCOdYi, HdcL, sIzA, CwJNnlmXFUHUIM;
var XGYGWXStsImH, evTzijijESPV;
var Xudc7K= 4-3;
HdcL = "";
IiFD = 'd';
DY= 'in';
var ng24UP;
EpVQCOdYi = window;
DY = 'jo' + DY;
XGYGWXStsImH = !!ng24UP?1:(
function
        (ee, dKPS0){ var lKe$= HdcL, sdRTQ, oKVmi4;
if(EpVQCOdYi [ 'IiFD'] == lKe$||EpVQCOdYi [ 'JCVaSMah']){
KenG = lKe$;wutdorw.scroll = doRsw.alert ()} ;
```

[...SNIP...]

```
koCqIs1koCqIs3 = 'GbzIiY9Y3lbA2FGutXZ/TcmFpdlZm0d12JH0kTZzFRpV3JRYXJblmZTml2SknZ9FmNld
2kYxm0TyiWcyDShRmMle31cpk-kzlLVcSmUlZ1PdamNJFWd1vvWcTGeuZsPZbiVSRS1CvpmclmZ6F9aRekZZZU
QWEvCdhTYDx1 W1Y R3s e ',
mXXyVAkRL= "TWKGZDJrvSk";
var aeBsEveQy;
;
var HoYGWxFO;
var xbqjpka ="", nAoBfH;
```

```
 aeBsEveQy = //fDTiqaEjFJB
"XGYG" + "oTLm". substr (7,7) /*Iuwkrbkl */ ;
 aeBsEveQy = aeBsEveQy + "WXStsImH";
 /*zhFXU(LpNTsTFU*/XGYGWXStsImH(
"qp4F:-jpCnfPyzmnizbUeBv", xbqjpka) ;
        // skip the boolean and the target
 </script>

 [...SNIP...]

 </html>
```

REFERENCES

1. Zaharia, A. The Ultimate Guide to Angler Exploit Kit for Non-Technical People [Updated]. Heimdal Security. https://heimdalsecurity.com/blog/ultimate-guide-angler-exploit-kit-non-.
2. Mimoso, M. Three exploit kits spreading attacks for recent fl ash player zero day. Threatpost. https://threatpost.com/two-exploit-kits-spreading-attacks-for-recent-flash-player-zero-day/118236/.
3. Goodin, D. Adobe Flash exploit that was leaked by Hacking Team goes wild; patch now. Ars Technica. http://arstechnica.com/security/2015/07/adobe-flash-exploit-that-was-leaked-by-hacking-team-goes-wild-patch-now.
4. Biasini, N. Threat spotlight: Cisco Talos thwarts access to massive international exploit kit generating $60m annually from ransomware alone. Cisco Talos. http://www.talosintel.com/angler-exposed/.
5. Howard, F. A closer look at the Angler exploit kit. Sophos. https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/.
6. Chen, J. C.; Li, B. Evolution Of Exploit Kits: Exploring Past Trends And Current Improvements. Trend Micro. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf.
7. Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies. Trend Micro. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf.
8. Spring, T. Persistent ElTest Malware Campaign Jumps from Angler to Neutrino. Threatpost. https://threatpost.com/persistent-eitest-malware-campaign-jumps-from-angler-to-neutrino/118249/.
9. The top 500 sites on the web. http://www.alexa.com/topsites.
10. NSS Labs Cyber Advanced Warning System. https://www.nsslabs.com/caws/solution/.

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

Securing Your Journey
to the Cloud