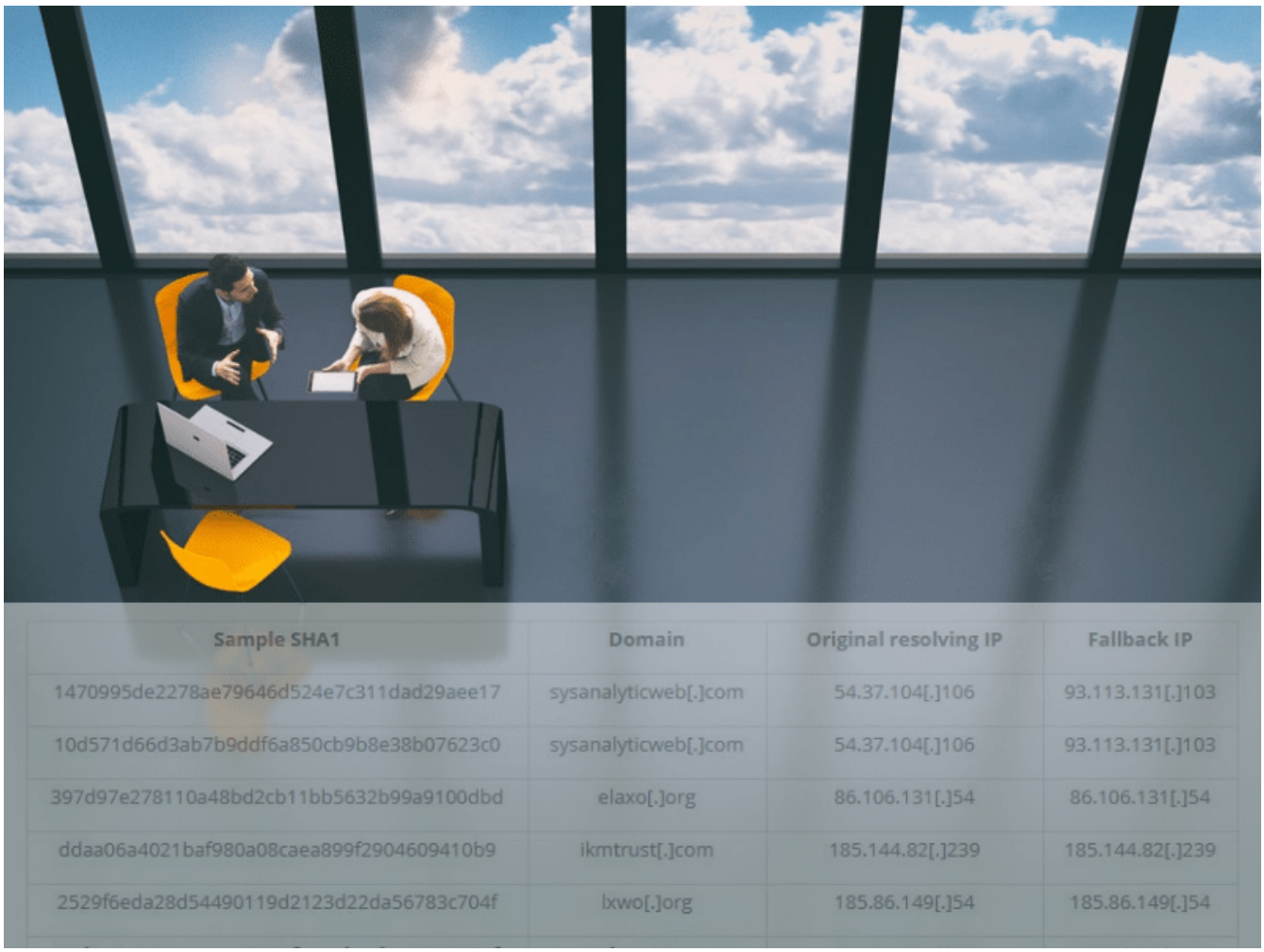
APT28 Rollercoaster: The Lowdown on Hijacked LoJack

lastline.com/labsblog/apt28-rollercoaster-the-lowdown-on-hijacked-lojack/

May 31, 2018



Sample SHA1	Domain	Original resolving IP	Fallback IP
1470995de2278ae79646d524e7c311dad29aee17	sysanalyticweb[.]com	54.37.104[.]106	93.113.131[.]103
10d571d66d3ab7b9ddf6a850cb9b8e38b07623c0	sysanalyticweb[.]com	54.37.104[.]106	93.113.131[.]103
397d97e278110a48bd2cb11bb5632b99a9100dbd	elaxo[.]org	86.106.131[.]54	86.106.131[.]54
ddaa06a4021baf980a08caea899f2904609410b9	ikmtrust[.]com	185.144.82[.]239	185.144.82[.]239
2529f6eda28d54490119d2123d22da56783c704f	lxwo[.]org	185.86.149[.]54	185.86.149[.]54

Posted by David Wells, Stefano Ortolani and Luukas Larinkoski ON MAY 31, 2018

Recently, the ASERT team at Arbor Networks, published a report on an old version of the Absolute Software product, Absolute LoJack for laptops, being illicitly modified by suspected APT28 actors. The LoJack implant, previously known as Computrace and brought into the spotlight in 2014 at Black Hat USA because it was enabled on some brand new laptops, is an anti-theft technology used in modern laptops to allow remote tracing, data deletion, and system lockdown.

Based on information from a number of reports, ASERT estimates with moderate confidence that the APT28 group, also known as Fancy Bear, has maliciously modified and deployed Absolute LoJack samples to support its own campaigns against government and defense-related contractors. (See the advice from Absolute Software regarding these modified samples.) As sophisticated implants often reveal non-trivial dynamic behaviors, we began an investigation process to analyze this threat in more detail.

A New Sample

From the IOCs in the ASERT report, we hunted through our knowledge base for additional samples using the search query below:

```
code_hash: '21B04C7DF33277B9927D0D3E3ADC545D' AND user_agent: 'Mozilla/4.0 (compatible;
```

```
MSIE 6.0;)' AND NOT domain: 'search.namequery.com'
```

The code hash search term allowed us to query for all LoJack implants. We filtered on user agent while removing the resolved domain used by all legitimate implants. The search uncovered a new and previously unmentioned sample, below (see Figure 1 for the analysis overview):

```
SHA1: 09d2e2c26247a4a908952fee36b56b360561984f
Compilation time: 2008-04-01 19:35:07
C&C server: webstp[.]com
```

This new sample was detected for the first time in the second half of 2017, the sample relies on a previously unknown C&C server: the webstp[.]com domain originally resolved to the IP address 185.94.191[.]65, but was later sinkholed at sinkhole.tigersecurity.pro via 91.134.203[.]113 and later 54.36.134[.]247.

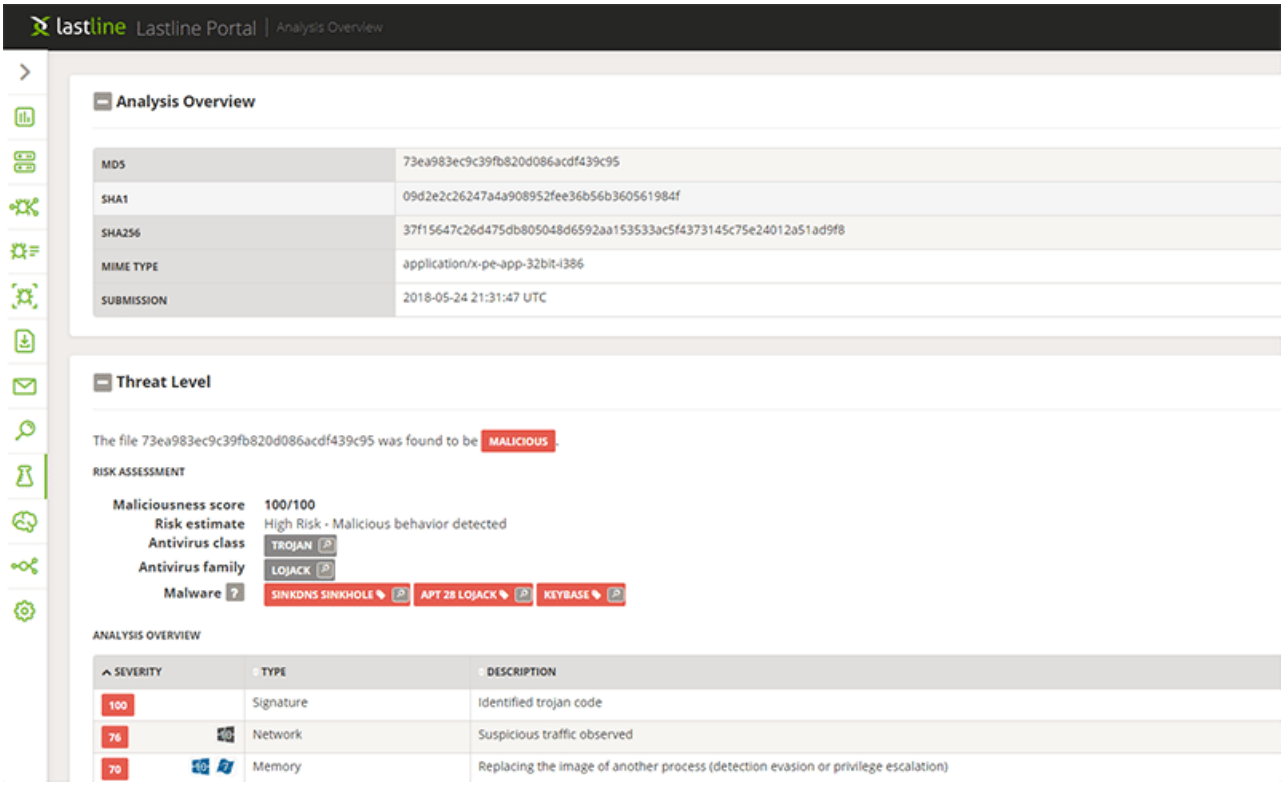


Figure 1: Analysis overview of the newly discovered hijacked LoJack sample.

Our investigation started by focusing on that specific domain and IP association. While we had no reputation information related to the IP 185.94.191[.]65, whois historical data showed that webstp[.]com had been registered on August 11, 2017 with the hosting company ititch[.]com (Figure 2).

WHOIS DATE	REGISTRAR NAME
11 Aug 2017	PDR Ltd. d/b/a PublicDomainRegistry.com

REGISTRANT CONTACT
Name: Boleslav Krejci
Address: Za Strasnickou vozovno 13421, Prague, Prague, 10000, Czech Republic
Email: bolekrejci@centrum.cz
Phone: +420.420260695632

TECHNICAL CONTACT
Name: Boleslav Krejci
Address: Za Strasnickou vozovno 13421, Prague, Prague, 10000, Czech Republic
Email: bolekrejci@centrum.cz
Phone: +420.420260695632

NAME SERVERS
ns1.ititch.com
ns2.ititch.com
ns3.ititch.com
ns4.ititch.com

Figure 2: Registration details for webstp.com before sinkholing (from whoxy.com).

In their own words:

> "IT Itch is different. We're all about helping people, businesses and activist groups keep their digital identity anonymous, their online data private and their websites always online. We're doing this by actively ignoring and impeding digital data requests and take-down notices, and we're pretty good at it – we have a 100% non-compliance rate. We're also helping domain name owners and website operators understand more about data privacy protection, and offering products and services designed to keep your identity secret, such as anonymous web hosting and private domain registration."

Whether intentionally or not, this desire to support internet freedoms has attracted cyberthreat actors because of the operational anonymity and bulletproof infrastructure.

The Fallback Revelation

During our investigation, we decided to verify whether we could detect other hijacked LoJack samples being used in the wild. As the traffic from hijacked agents is otherwise indistinguishable from legitimate agents, we deployed a network signature to monitor HTTP traffic with the same distinct User-Agent header, but connecting to other (non-legitimate) domains. Unfortunately, this approach quickly proved to be prone to false positives; in particular, in a small number of legitimate LoJack interactions, the contacted host of the HTTP request was a plain IP address instead of a domain name (see Figure 3).

Figure 3: A legitimate LoJack network interaction using the IP address as contacted hostname.

The fact that a legitimate sample was including this fallback mechanism led us to wonder whether the malicious binary was doing the same. As Figure 4 shows, that was indeed the case: it turns out Computrace samples embed both a XORed IP address as well as a XORed domain. The XORed IP address is used as a backup communication channel when domain callout fails (the logic can be seen in Figure 5).

```
.cdata:0040606B                 db 0B5h ; ¦
.cdata:0040606C                 db 0E5h ; s
.cdata:0040606D                 dd 0F40AEB0Ch           ; XORed IP_ADDRESS 185.94.191.65
.cdata:00406071                 db 0C2h ; -             ; XORed domain webstp.com
.cdata:00406072                 db 0D0h ; -
.cdata:00406073                 db 0D7h ; +
.cdata:00406074                 db 0C6h ; ¦
.cdata:00406075                 db 0C1h ; -
.cdata:00406076                 db 0C5h ; +
.cdata:00406077                 db  9Bh ; ¢
.cdata:00406078                 db 0D6h ; +
.cdata:00406079                 db 0DAh ; +
.cdata:0040607A                 db 0D8h ; +
.cdata:0040607B                 db 0B5h ; ¦
.cdata:0040607C                 db 0B5h ; ¦
.cdata:0040607D                 db 0B5h ; ¦
.cdata:0040607E                 db 0B5h ; ¦
.cdata:0040607F                 db 0B5h ; ¦
.cdata:00406080                 db 0B5h ; ¦
.cdata:00406081                 db 0B5h ; ¦
.cdata:00406082                 db 0B5h ; ¦
.cdata:00406083                 db 0B5h ; ¦
.cdata:00406084                 db 0B5h ; ¦
.cdata:00406085                 db  0Ah
```

Figure 4: The XORed IP and domain name.

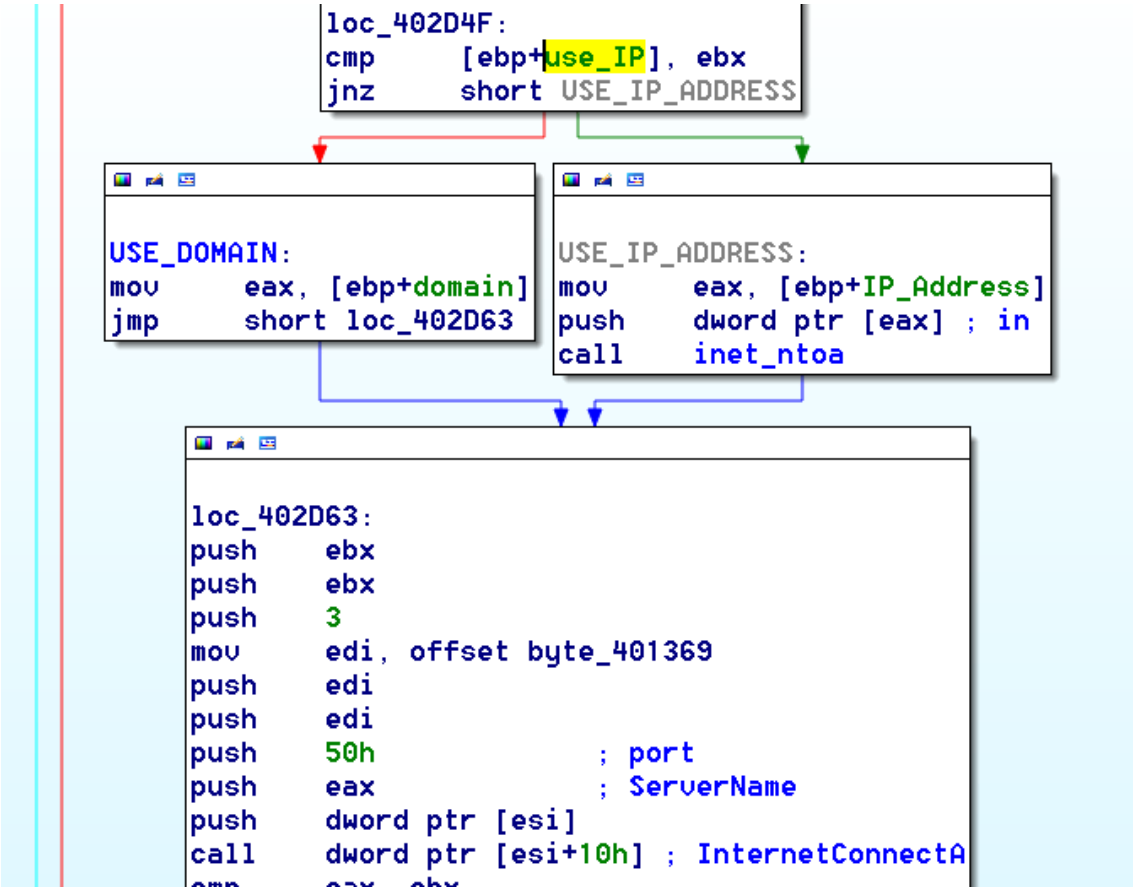


Figure 5: The logic used to decide when to fallback to an IP address.

We also checked all other hijacked LoJack implants, and in all cases, the binary included a fallback IP, meaning that in all cases the implant would have been able to connect to the C&C regardless of whether the domain had been sinkholed or blacklisted. Only in two cases, the fallback IP address did not match the address pointed to by the domain. Table 1 shows detailed network IOCs for all known hijacked LoJack samples.

Sample SHA1	Domain	Original resolving IP	Fallback IP
1470995de2278ae79646d524e7c311dad29aee17	sysanalyticweb[.]com	54.37.104[.]106	93.113.131[.]103
10d571d66d3ab7b9ddf6a850cb9b8e38b07623c0	sysanalyticweb[.]com	54.37.104[.]106	93.113.131[.]103
397d97e278110a48bd2cb11bb5632b99a9100dbd	elaxo[.]org	86.106.131[.]54	86.106.131[.]54
ddaa06a4021baf980a08caea899f2904609410b9	ikmtrust[.]com	185.144.82[.]239	185.144.82[.]239
2529f6eda28d54490119d2123d22da56783c704f	lxwo[.]org	185.86.149[.]54	185.86.149[.]54
09d2e2c26247a4a908952fee36b56b360561984f	**webstp[.]com**	**185.94.191[.]65**	**185.94.191[.]65**

Table 1: Hijacked LoJack samples and their C&C infrastructure (including the fallback IP). In bold the sample we uncovered.

Attribution

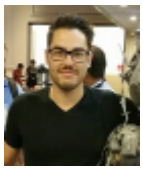
We can assert with high confidence that this specific hijacked Absolute LoJack for laptops sample appears to be related to the campaign recently unveiled by Arbor Networks. Our reasoning follows:

- The domain webstp[.]com is associated to an Absolute LoJack agent utilizing the exact same compile time of other hijacked LoJack samples, thus matching the same criteria used to cluster the original artifacts.
- The domain sysanalyticweb[.]com and webstp[.]com share the same registrar, ititch[.]com, a company claiming to provide bulletproof hosting, and used in other APT28 campaigns.
- The domain in the registrant email address for webstp[.]com is centrum[.]cz, which appears frequently in other registrant email addresses of domains linked to previous APT28 campaigns associated with ititch[.]com.
- The Absolute LoJack for laptops agent connecting to webstp[.]com has been seen in the wild during the same time frame of all other samples.

Conclusions

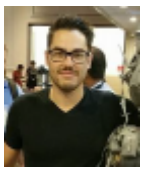
In this blog post, we further analyzed the C&C infrastructure used by the samples of Absolute LoJack for laptops illicitly modified by APT28. We unveiled a new sample submitted from organizations with a consistent victimology to other LoJack targets and domains that are part of the C&C infrastructure. We also discovered that all Absolute LoJack for laptops samples had a fallback mechanism to increase their robustness against sinkholes. This infrastructure used in our new sample is linked to pro-European Union companies and/or ex-Soviet Union states. We will continue to publish new IOCs in this blog for the LoJack campaign as future submissions appear.

- About
- Latest Posts



David Wells

David Wells is a Malware Reverse Engineer at Lastline with 4 years experience working in malware, botnet, and exploitation research. Previously he worked at Integral Ad Science and independent contracting for botnet tracking and exploitation research. His background consists of Windows internals with emphasis on cryptography and protocol reverse engineering for botnet/C&C research.



Latest posts by David Wells (see all)

- APT28 Rollercoaster: The Lowdown on Hijacked LoJack - May 31, 2018
- When Scriptlets Attack: Excel's Alternative to DDE Code Execution - December 7, 2017

- About
- Latest Posts

Stefano Ortolani

Stefano Ortolani is Director of Threat Intelligence at Lastline. Prior to that he was part of the research team in Kaspersky Lab in charge of fostering operations with CERTs, governments, universities, and law enforcement agencies. Before that he earned his Ph.D. in Computer Science from the VU University Amsterdam.

Latest posts by Stefano Ortolani (see all)

- Evolution of Excel 4.0 Macro Weaponization - June 2, 2020
- InfoStealers Weaponizing COVID-19 - May 11, 2020
- Nemty Ransomware Scaling UP: APAC Mailboxes Swarmed by Dual Downloaders - February 18, 2020

- About
- Latest Posts

Luukas Larinkoski

Luukas Larinkoski is a Network Threat Analyst at Lastline. He enjoys uncovering and defending against both new and emerging network threats, and spends most of his time researching and developing systems for protecting customer networks. His research interests include network anomaly detection and security event correlation.

Latest posts by Luukas Larinkoski (see all)

- APT28 Rollercoaster: The Lowdown on Hijacked LoJack - May 31, 2018
- A Wild Port Scan Appears. What now? - May 9, 2018

Tags:

Andy Norton, APT28, attribution, C&C infrastructure, Computrace, David Wells, Fancy Bear, Lastline Labs, LoJack implant, Luukas Larinkoski, Stefano Ortolani