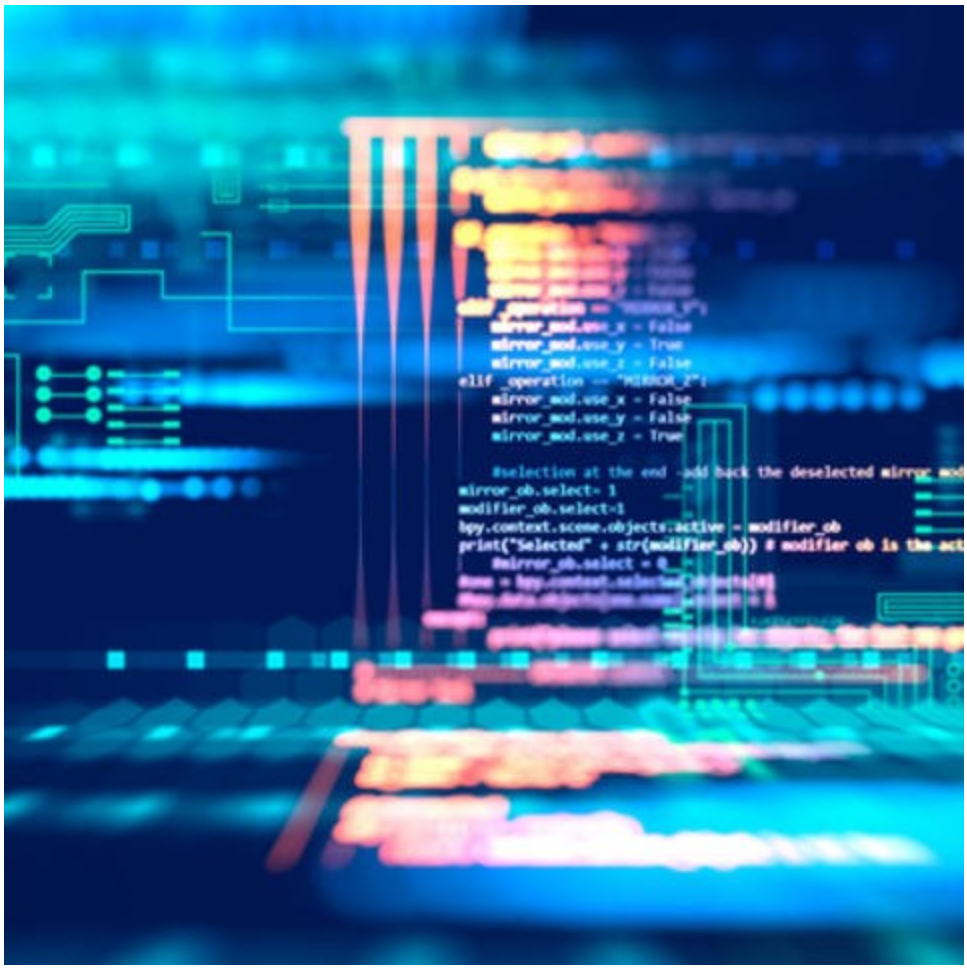
Lojack Becomes a Double-Agent

asert.arbornetworks.com/lojack-becomes-a-double-agent/



by ASERT Team on May 1st, 2018

Executive Summary

ASERT recently discovered Lojack agents containing malicious C2s. These hijacked agents pointed to suspected Fancy Bear (a.k.a. APT28, Pawn Storm) domains. The InfoSec community and the U.S. government have both attributed Fancy Bear activity to Russian espionage activity. Fancy Bear actors typically choose geopolitical targets, such as governments and international organizations. They also target industries that do business with such organizations, such as defense contractors. Lojack, formally known as Computrace, is a legitimate laptop recovery solution used by a number of companies to protect their assets should they be stolen. Lojack makes an excellent double-agent due to appearing as legit software while natively allowing remote code execution. Although the initial intrusion vector for this activity remains unknown, Fancy Bear often utilizes phishing email to deliver payloads. ***NOTE:*** *Arbor APS enterprise security products detect and block on all activity noted in this report.*

Key Findings

- ASERT researchers identified Lojack agents containing command and control (C2) domains likely associated with Fancy Bear operations.

- Proof of concept in using Lojack as a backdoor or intrusion vector date back to 2014. Its continued use suggest attackers could have used it in long-running operations.
- Initially, the Lojack agents containing rogue C2 had low Anti-Virus (AV) detection which increased the probability of infection and subsequent successful C2 communication.
- The distribution mechanism for the malicious Lojack samples remains unknown. However, Fancy Bear commonly uses phishing to deliver malware payloads as seen with Seduploadin late 2017.

UPDATE

- **May 3, 2018 –** After the disclosure of the malicious Lojack binaries, many Anti-Virus vendors have been quick to respond in properly marking samples as "malware" and "DoubleAgent", rather than "Riskware" or "unsafe" (**Figure 2**).
- **May 4th 2018 –** UPDATE FROM ABSOLUTE SOFTWARE:

  "The analysis of the samples provided by Arbor shows all were based on an illicitly modified old version of the LoJack agent from 2008 and no customers or partners have been impacted. For customers who wish to confirm no legacy agents are present in their environment, we have published an advisory with steps to verify all installed agents are legitimate copies of the LoJack product.
- **May 9th 2018 –** Disclaimer:

  Prior reports have misidentified LoJack instead of Absolute LoJack for Laptops, also known as Computrace. LoJack for Laptops and Computrace are products of Absolute, not LoJack or CalAmp.

Lojack Summary

Absolute Software, the creator of Lojack, says on its website (https://www.absolutelojack.com/) that the agent can locate and lock a device remotely. Additionally, it can delete files, making it an effective laptop theft recovery and data wiping platform. Lojack can survive hard drive replacements and operating system (OS) re-imaging. The agent achieves this persistence through a modular design as noted by Vitaliy Kamlyuk, Sergey Belov, and Anibal Sacco in a presentation at Blackhat, 2014 (**Figure 1**):

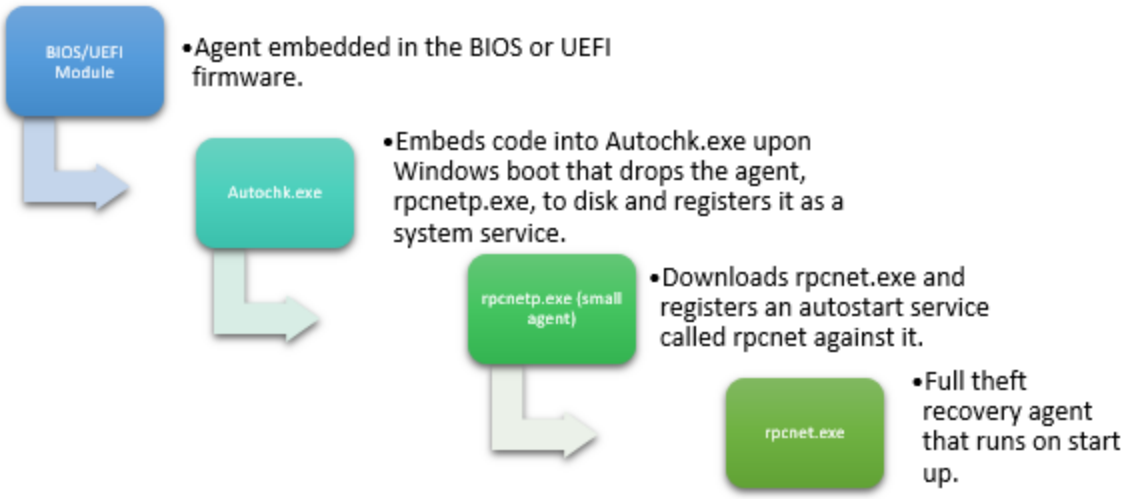


Figure 1: Lojack persistence mechanism (Paraphrased from https://www.blackhat.com/docs/us-14/materials/us-14-Kamluk-Computrace-B…).

The aforementioned researchers suggest the binary modification of the "small agent" is trivial. The Lojack agent protects the hardcoded C2 URL using a single byte XOR key; however, according to researchers it blindly trusts the configuration content. Once an attacker properly modifies this value then the double-agent is ready to go. This is not the only aspect that makes Lojack an appealing target. Attackers are also concerned about AV detection. Looking on VirusTotal, some anti-virus vendors flag Lojack executables as ”unsafe”, but as noted as of May 3, many AV now flag the binaries as malware and DoubleAgent (**Figure 2**).

Detection | Details | Relations | Behavior | Community 5

Ad-Aware	Trojan.GenericKD.30704825	AegisLab	Uds.Dangerousobject.Multi!c
AhnLab-V3	Trojan/Win32.Agent.C2487603	ALYac	Backdoor.DoubleAgent.A
Arcabit	Trojan.Generic.D1D484B9	Avira	TR/RedCap.hjqdd
BitDefender	Trojan.GenericKD.30704825	Bkav	W32.eHeur.Malware11
Cylance	Unsafe	Cyren	W32/Backdoor.GV.gen!Eldorado
eScan	Trojan.GenericKD.30704825	F-Prot	W32/Backdoor.GV.gen!Eldorado
F-Secure	Trojan.GenericKD.30704825	Fortinet	W32/DoubleAgent.C!tr.bdr
GData	Trojan.GenericKD.30704825	Ikarus	Trojan.Win32.Falojak
Kaspersky	Backdoor.Win32.DoubleAgent.c	MAX	malware (ai score=94)
McAfee	RDN/Generic BackDoor	McAfee-GW-Edition	BehavesLike.Win32.Injector.lh
Microsoft	Trojan:Win32/Falojak	nProtect	Backdoor/W32.DoubleAgent.17408
Sophos AV	Troj/DblAgnt-B	Sophos ML	heuristic
Symantec	Trojan.Gen.6	TrendMicro	TROJ_FRS.0NA103E318
TrendMicro-HouseCall	TROJ_FRS.0NA103E318	VIPRE	Trojan.Win32.Generic!BT

Figure 2: Virustotal AV Report of cf45ec807321d12f8df35fa434591460

Originally, the low AV detection, allowed the attacker to hide in plain sight, an effective double-agent. The attacker simply needs to stand up a rogue C2 server that simulates the Lojack communication protocols. Finally, Lojack's "small agent" allows for memory reads and writes which grant it remote backdoor functionality when coupled with a rogue C2 server.

Lojack Double-Agent

ASERT has identified five Lojack agents (rpcnetp.exe) pointing to 4 different suspected domains. Fancy Bear has been tied to three of the domains in the past.

Hash	Compilation Time	Size in Bytes	Rogue C2 Servers	AV Detection on VT
f1df1a795eb784f7bfc3ba9a7e3b00ac	2008-04-01 19:35:07	17,408	sysanalyticweb[.]com	2/67
6eaa1ff5f33df3169c209f98cc5012d0	2008-04-01 19:35:07	17,408	sysanalyticweb[.]com	4/66
f3c6e16f0dd2b0e55a7dad365c3877d4	2008-04-01 19:35:07	17,408	elaxo[.]org	3/62
cf45ec807321d12f8df35fa434591460	2008-04-01 19:35:07	17,408	ikmtrust[.]com	2/64
f391556d9f89499fa8ee757cb3472710	2008-04-01 19:35:07	17,408	lxwo[.]org	9/65

Table 1: Lojack Double-Agents on VirusTotal

Binary Comparisons

ASERT believes all these binaries are rpcnetp.exe (small agent) due to the following characteristics:

- Size matching: 17,408 bytes
- Yara match on either:
  - "TagId" and "rpcnetp.exe"
  - Set of op codes
- Matching export function "rpcnetp" in the binaries.

After confirming the stage of the Lojack agent, binary comparison analysis confirmed that they were legitimate Lojack samples. The comparison also highlighted that the attacker did not graft additional functionality into the binary. ASERT used the presence of search.namequery[.]com in the binary and the yara rule to identify legitimate Lojack samples. Lojack's Absolute Software Corp. owns search.namequery[.]com; we have no

evidence the legitimate site has been used for nefarious purposes. **NOTE:** All samples, both rogue and the two “clean” samples (below), matched 100% based on Diaphora’s function matching algorithm. “Clean” Samples:

1. e78e3b0171b189074d2539c7baaa0719
2. ac1a85d3ca1b6265cad4ed41b696f9b7

Only the presence of the rogue C2's make the samples in **Table1** malicious. The attackers are merely hijacking the communication used by Lojack, thereby granting themselves backdoor access to machines running the software.

Fancy Bear Attribution

ASERT assesses with moderate confidence that the rogue Lojack agents are attributed to Fancy Bear based on shared infrastructure with previous operations. The following domains, extracted from the rogue Lojack agents trace back to Fancy Bear operations:

1. elaxo[.]org
2. ikmtrust[.]com
3. lxwo[.]org
4. sysanalyticweb[.]com (**Figure 3** & **Figure 4**)

Researchers from Jigsaw Security, based on leads from Talos in late 2017, traced the domains elaxo[.]org and ikmtrust[.]com and the tool Seduploa d, to a Fancy Bear operation. The domain lxwo[.]org appeared in a blog post from Threat Intel Recon that resolved to an IP address within a document attributed to Fancy Bear. The rogue Lojack samples containing the sysanalyticweb[.]com domains were only recently spotted in the wild (April 2018). Despite the hijack of this software being a publicly known tactic, there are many similarities in the binary comparisons (above) and infrastructure analysis (below) that increase the probability it is the same actor(s):

- All the listed domains are associated with the same Lojack agent utilizing the same compile time.
- The domains in question all contain nonsensical Registrant information where the actor tends to copy/paste the same information in multiple fields.
- Each domain includes a Registrant Name (often a nonsensical word), but additionally includes a similar word in the Registrant Organization field.
    - This is interesting because that is a field that is often skipped when a Registrant Name is present, but this actor(s) regularly utilizes both fields

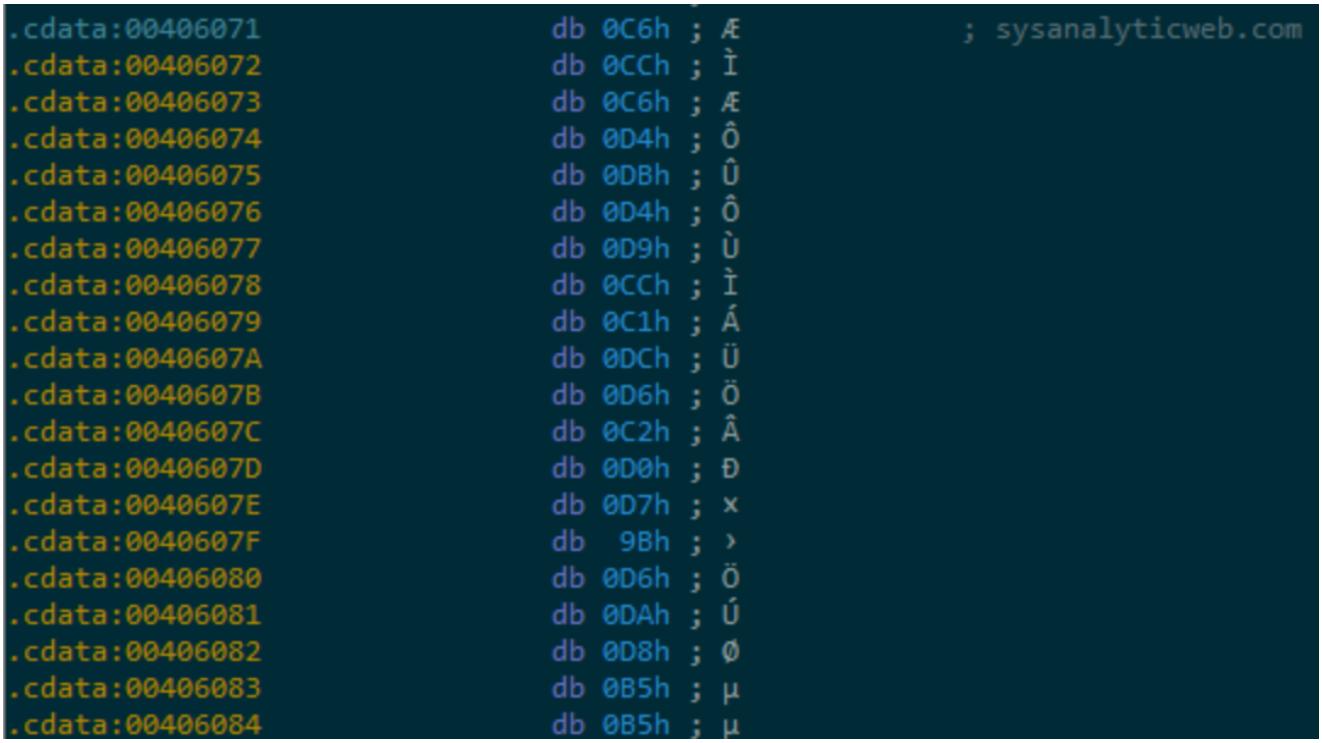


Figure 3. XORed C2 Server - NETSCOUT

```
POST / HTTP/1.1
Host: sysanalyticweb.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;)
TagId: 0
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date:  ,  Apr 2018  GMT
Server: Apache/2.4.6 (CentOS) mod_wsgi/3.4 Python/2.7.5
TAGID:
X-Frame-Options: SAMEORIGIN
Content-Length: 15
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

~...........^ ~
```

Figure 4. Live (April 2018) C2 - NETSCOUT

Conclusion & Recommendations

Hijacking legitimate software is a common enough tactic for malicious actors. A key factor making this activity so devious is the malicious Lojack samples were simply labeled "unsafe”, "suspicious", or "DangerousObject", rather than malware. As a result, rogue Lojack samples could fly under the radar and give attackers a stealthy backdoor into victim systems. ASERT recommends scanning for rogue Lojack agents using the Yara signature listed in the Appendix (below) and blocking the domains contained within this blog.

Appendix: Yara Signature

```
rule ComputraceAgent
{
 meta:
     description = "Absolute Computrace Agent Executable"
     thread_level = 3
     in_the_wild = true
 strings:
     $a = {D1 E0 F5 8B 4D 0C 83 D1 00 8B EC FF 33 83 C3 04}
     $mz = {4d 5a}
     $b1 = {72 70 63 6E 65 74 70 2E 65 78 65 00 72 70 63 6E 65 74 70 00}
     $b2 = {54 61 67 49 64 00}
 condition:
     ($mz at 0 ) and ($a or ($b1 and $b2))
}
```

Code Snippet 1: Yara signature to detect computrace/Lojack agent (Retrieved from https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Comp…)

Posted In

- Advanced Persistent Threats
- Malware

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.