Fidelis Cybersecurity®

DATASHEET

Fidelis Network® Web Sensor

Prevent Threats and Data Loss in Proxied Web Traffic

Optimize User Experience While Preventing Threats and Data Loss

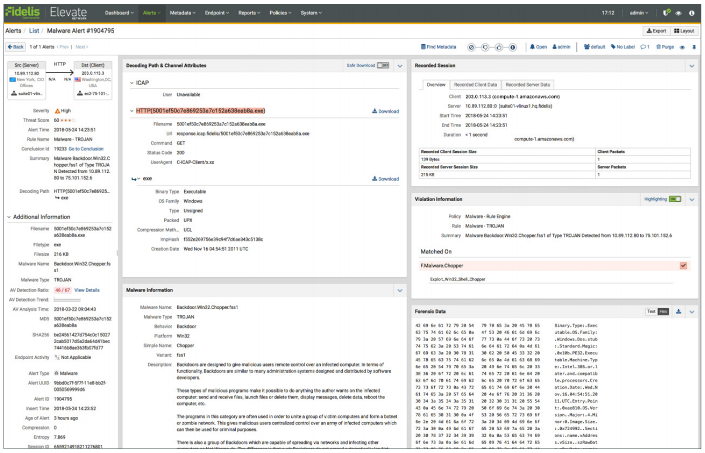
User web experience is critical, and when threats or data loss are detected, providing informative web pages on policy violations is important. While many defenses can drop sessions, the user web experience is less than optimal and may lead to IT support calls. Fidelis Web Sensor integrates with ICAP (or S-ICAP) compatible network devices and web proxies to prevent threats and data loss in web requests and replies, including encrypted web traffic if inspected by your web proxy.

Product Overview

The Fidelis Web Sensor is an integral part of Fidelis Network® that comprises of several sensors including the Direct, Internal, Mail, and Web Sensors. Fidelis Network provides deep content visibility into network, email, and web proxy traffic to reveal malicious payloads or malware in web requests and detect any data leaving your network in outbound web content. The Fidelis Network Web Sensor can be connected to an ICAP/S-ICAP (Secure ICAP) capable network or web proxy device that can pass web requests and replies over ICAP / S-ICAP for content analysis.

The Fidelis Web Sensor will analyze all received content and can direct the external network device or web proxy to prevent web requests or replies, or redirect the user away to informative policy violation web pages. Since many web proxies support the decryption of encrypted traffic, the Fidelis Web Sensor can receive decrypted web content over ICAP / S-ICAP for inspection. This enables the Web Sensor to analyze all web content — even over encrypted web sessions.

Web traffic is analyzed using Fidelis' proprietary threat intelligence and Malware Detection Engine — including signature, heuristic, sandboxing, and machine learning analysis — to identify any inbound and outbound threats such as malware, malicious attachments, and data leakage in real-time.



Alerts / List / Malware Alert #1904795

1 of 1 Alerts < Prev | Next >

Src (Server)	HTTP	Dst (Client)
10.89.112.80 New York, CIO Offices suite01-vlin...	N/A → N/A	203.0.113.3 Washington,DC, USA ec2-75-101-...

Severity: High
Threat Score: 60
Alert Time: 2018-05-24 14:23:51
Rule Name: Malware - TROJAN
Conclusion Id: 19233 Go to Conclusion
Summary: Malware Backdoor.Win32.Chopper.fss1 of Type TROJAN Detected from 10.89.112.80 to 75.101.152.6
Decoding Path: HTTP(5001ef50c7e86925... ↳ exe

Additional Information
Filename: 5001ef50c7e869253a7c152a638eab8a.exe
Filetype: exe
Filesize: 216 KB
Malware Name: Backdoor.Win32.Chopper.fss1
Malware Type: TROJAN
AV Detection Ratio: 46 / 67 View Details
AV Detection Trend:
AV Analysis Time: 2018-03-22 09:04:43
MD5: 5001ef50c7e869253a7c152a638eab8a
SHA256: be24561427d754c0c15027 2cab5017d5a2da64d41bec 74416b8ae363fb07fd77
Endpoint Activity: Not Applicable
Alert Type: Malware
Alert UUID: 9bbd0c7f-5f7f-11e8-bb2f-0050569999d6
Alert ID: 1904795
Insert Time: 2018-05-24 14:23:52
Age of Alert: 3 hours ago
Compression: 0
Entropy: 7.869
Session ID: 6559214918211276801

Decoding Path & Channel Attributes

ICAP
User: Unavailable

HTTP(5001ef50c7e869253a7c152a638eab8a.exe)
Filename: 5001ef50c7e869253a7c152a638eab8a.exe
Url: response.icap.fidelis/5001ef50c7e869253a7c152a638eab8a.exe
Command: GET
Status Code: 200
UserAgent: C-ICAP-Client/x.xx

exe
Binary Type: Executable
OS Family: Windows
Type: Unsigned
Packed: UPX
Compression Meth...: UCL
ImpHash: f552e269756e39c94f7d6ae343c5138c
Creation Date: Wed Nov 16 04:54:51 2011 UTC

Malware Information
Malware Name: Backdoor.Win32.Chopper.fss1
Malware Type: TROJAN
Behavior: Backdoor
Platform: Win32
Simple Name: Chopper
Variant: fss1
Description: Backdoors are designed to give malicious users remote control over an infected computer. In terms of functionality, Backdoors are similar to many administration systems designed and distributed by software developers.

These types of malicious programs make it possible to do anything the author wants on the infected computer: send and receive files, launch files or delete them, display messages, delete data, reboot the computer, etc.

The programs in this category are often used in order to unite a group of victim computers and form a botnet or zombie network. This gives malicious users centralized control over an army of infected computers which can then be used for criminal purposes.

There is also a group of Backdoors which are capable of spreading via networks and infecting other

Recorded Session
Client: 203.0.113.3 (compute-1.amazonaws.com)
Server: 10.89.112.80:0 (suite01-vlinux1.hq.fidelis)
Start Time: 2018-05-24 14:23:51
End Time: 2018-05-24 14:23:51
Duration: < 1 second
compute-1.amazonaws.com)

Recorded Client Session Size	Client Packets
139 Bytes	1
Recorded Server Session Size	Server Packets
215 KB	1

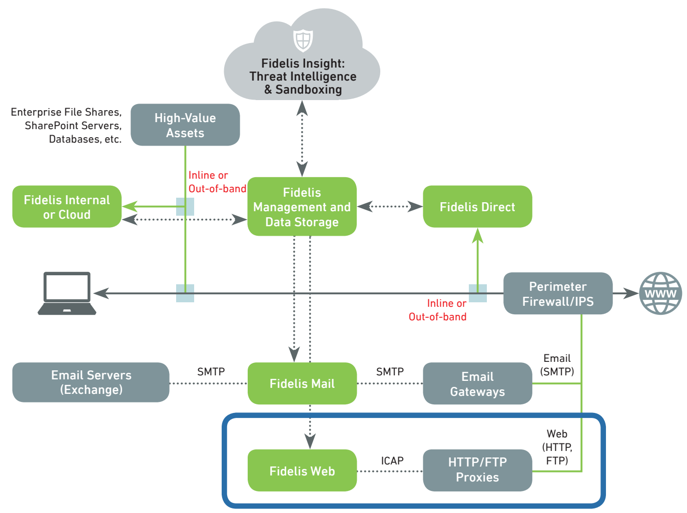
Violation Information
Policy: Malware - Rule Engine
Rule: Malware - TROJAN
Summary: Malware Backdoor.Win32.Chopper.fss1 of Type TROJAN Detected from 10.89.112.80 to 75.101.152.6

Matched On
F.Malware.Chopper ✓
Exploit_Win32_Shell_Chopper

Forensic Data

```
42 69 6e 61 72 79 20 54   79 70 65 3a 20 45 78 65   Binary.Type:.Exec
63 75 74 61 62 6c 65 0a   4f 53 20 46 61 6d 69 6c   utable.OS.Family:
79 3a 20 57 69 6e 64 6f   77 73 0a 44 6f 73 20 73   .Windows.Dos.stub
74 75 62 3a 20 53 74 61   6e 64 61 72 64 0a 4d 61   :.Standard.Magic:
67 69 63 3a 20 30 78 31   30 62 20 50 45 33 32 20   .0x10b.PE32.Execu
45 78 65 63 75 74 61 62   6c 65 0a 4d 61 63 68 69   table.Machine.Typ
6e 65 20 54 79 70 65 3a   20 49 6e 74 65 6c 20 33   e:.Intel.386.or.l
38 36 20 6f 72 20 6c 61   74 65 72 20 61 6e 64 20   ater.and.compatib
63 6f 6d 70 61 74 69 62   6c 65 20 70 72 6f 63 65   le.processors.Cre
73 73 6f 72 73 0a 43 72   65 61 74 69 6f 6e 20 44   ation.Date:.Wed.N
61 74 65 3a 20 57 65 64   20 4e 6f 76 20 31 36 20   ov.16.04:54:51.20
30 34 3a 35 34 3a 35 31   20 32 30 31 31 20 55 54   11.UTC.Entry.Poin
43 0a 45 6e 74 72 79 20   50 6f 69 6e 74 3a 20 30   t:.0xae810.OS.Ver
78 61 65 38 31 30 0a 4f   53 20 56 65 72 73 69 6f   sion..Major:.4.Mi
6e 2e 20 4d 61 6a 6f 72   3a 20 34 09 4d 69 6e 6f   nor:0.Image.Size.
72 3a 30 0a 49 6d 61 67   65 20 53 69 7a 65 20 3a   :.0x724992..Secti
20 30 78 37 32 34 39 39   32 0a 0a 53 65 63 74 69   ons:.name.vAddres
6f 6e 73 3a 0a 6e 61 6d   65 09 76 41 64 64 72 65   s.vSize..szRawDat
```

Identify threats and data loss in proxy traffic



Fidelis Network Architecture

Fidelis Web Sensor provides threat and data loss prevention with informative policy violation details on web page redirects for an improved user web experience.

When to Add Fidelis Web Sensor to Your Network

The Fidelis Web Sensor goes beyond traditional web traffic monitoring tools by using patented technology to inspect and detect threats and data leakage buried deep within web content. While the Fidelis Network Direct and Internal Sensors detect threats across all ports and protocols, the Web Sensor ensures the prevention of threats and data loss for protocols traversing network devices or web proxies supporting ICAP/ S-ICAP. If your web proxy also supports network decryption, the Web Sensor is less disruptive and seamless to the enterprise than the combination of a Direct Sensor and a network decryption server. With the Fidelis Web Sensor you can:

- **Handle Decryption:** Many web proxy servers handle decryption which allows them to send unencrypted content to the Fidelis Web Sensor securely over S-ICAP with no risk of exposure. If the web proxy supports this feature, Fidelis Web Sensor can inspect all content, even encrypted network communications traversing your web proxy in a secure manner.
- **Enforce Prevention:** The Web Sensor can gracefully enforce prevention by redirecting the user to an internal web page to inform them of the security violation and company policies. This web page can be configured as needed within the enterprise and tailored to the specific reasons for the violation. Conversely when a Fidelis Direct or Internal Sensor prevents a similar web session, the user experience appears the same as a network failure to deliver web requests and may lead to IT support calls and a less than optimal user experience.

Configuration Options

The Web Sensor can be configured to handle prevention in one of two modes:

- **Dropping the Session:** The user will receive an error response from the ICAP / S-ICAP connected network or web proxy device. This is the less preferred response to users for policy violations.
- **Redirecting the User:** If the network device is a web proxy, it can redirect the user to a web page crafted and maintained by the enterprise for policy violations. This action would lead the user to a web page that informs the user of a security violation, company policies, or any pertinent message you wish to provide. The enterprise can create many such web pages and configure the response based on the details of any particular violation. The Fidelis Web Sensor chooses the correct web page redirection based on the policy violation and system configuration (i.e. malware alert, data loss prevention alert).

In each case, the response is performed by the network or web proxy device based on instructions provided by the Fidelis Web Sensor over the ICAP/ S-ICAP response. Prevention performance is dictated by the features of the network or web proxy device. In many cases the network or web proxy device can be configured to buffer the inbound or outgoing web request or reply and wait for an ICAP / S-ICAP response. When the web proxy is configured in this manner, prevention can be guaranteed.

What is ICAP* and RFC 3507?

ICAP, the Internet Content Adaption Protocol, is a protocol aimed at providing simple object-based content vectoring for HTTP services. ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients (i.e. network devices and web proxies) to pass HTTP messages to ICAP servers (i.e. Fidelis Web Sensor) for some sort of transformation or other processing ("adaptation").

The server executes its transformation service (i.e. threat and malware detection, data loss and theft prevention) on messages and sends back responses to the client, usually with modified messages. The adapted messages may be either HTTP requests or HTTP responses with the option of redirecting to web pages providing information for policy violations. S-ICAP is an encrypted communications version between ICAP clients and servers for data protection, often when web proxy servers decrypt and inspect encrypted traffic (i.e. SSL/TLS). ICAP also off-loads compute processing from ICAP clients to servers for optimization and performance.

Reference – http://www.icap-forum.org/documents/specification/rfc3507.txt

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.