F5 Security Operations Center

DATASHEET

What's Inside

Always on the Watch for You

Protecting e-commerce and online banking sites and their customers requires constant vigilance. Businesses must guard against online fraud and phishing attacks as well as continuously analyze threats and quickly respond to discovered malware and malicious activities. Organizations without ongoing global watch and expert fraud and malware analysis struggle to effectively counter fraud and may suffer serious business consequences as a result.

The F5 Security Operations Center (SOC) monitors global attack activities in real time, notifies customers of threats, and shuts down phishing proxies or drop zones to minimize their impact on businesses. It also:

- Houses an experienced team of security researchers and analysts who investigate new attacks throughout the world.
- Maintains up-to-date information on the latest malware, zero-day, and phishing attacks that target the financial service industry.
- Operates 24/7 to drive awareness of fraud threats that may pose immediate danger.

The F5 SOC is responsible for discovering a variety of noted threats—such as Eurograbber and several key zero-days threats—and works closely with law enforcement worldwide.

Key benefits

Ensure 24/7 threat monitoring and responses

Get peace of mind that an expert team with leading-edge technology is available 365 days a year and is monitoring and responding to security threats.

Shut down phishing sites efficiently

Shut down malicious sites or drop zones in hours and before malicious campaigns are executed.

Maintain up-to-date global threat intelligence

Get reports on the latest and most sophisticated attacks that may affect your business.

Effective malware analysis

Recognize and safeguard against sophisticated threats, including web injection, credential grabbing, man-in-the-browser (MITB), man-in-the-middle (MITM), session hijacking, password stealers, and more.

Start services easily

F5 SOC services can be easily set up and activated to support F5® WebSafe™ or MobileSafe™.

Security Operations Center—Services

The F5 Security Operations Center supplements F5 WebSafe and MobileSafe solutions for customer-protected online applications or URLs. SOC services provide scaling business capabilities that bring visibility to and protection against the mounting risk of advanced financial fraud, as well as extending corporate fraud and security teams with added expert assistance.

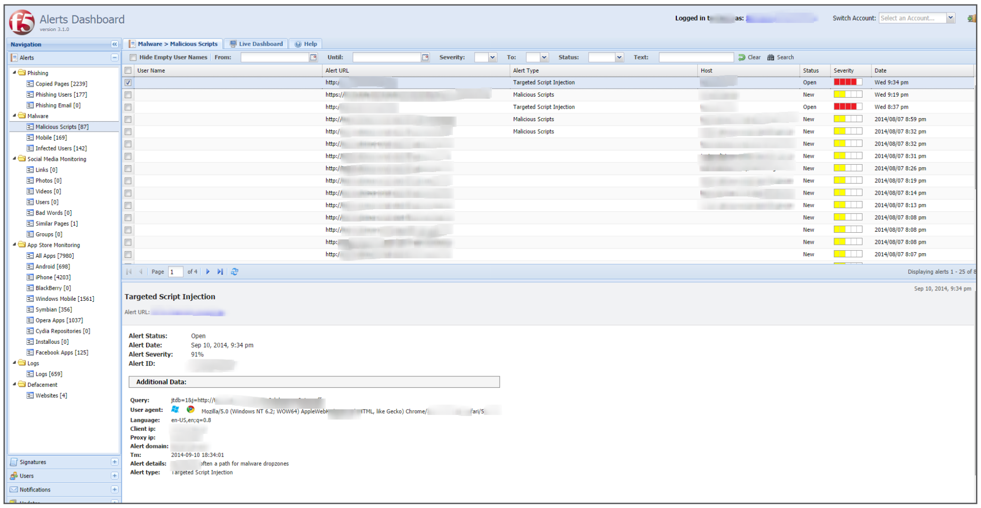
When an attack takes place, a SOC analyst contacts a client immediately to advise on the situation, discuss the potential threat level, and recommend actions to take. They also provide analysis and reports to help organizations take a proactive stance against cybercrime. With F5 SOC services, organizations are better able to deal with the threat of fraud on an organizational and technical level, and minimize fraud loss with early detection and rapid response.

Fraud team alerts and dashboard

The F5 SOC Web Fraud dashboard helps service administrators and fraud specialists stay on top of fraudsters targeting their business by enabling them to:

- Receive immediate notification and visibility into suspicious financial malware as well as phishing events targeting online banking customers.
- Log on to the cloud-hosted service from anywhere and using any browser to view all F5 WebSafe and MobileSafe alerts and monitor the details of threats targeting specific URLs in real time.
- Receive real-time fraud alerts through email and SMS.

The Web Fraud dashboard provides a comprehensive view of alerts and allows users to segment or search data by alert type, date, severity, status, and more. Users can drill down to specific details on each incident listed, including origin, proxy, referrer, user agent, and query.


Alerts Dashboard
version 3.1.0
Logged in t[redacted] as: [redacted]
Switch Account: Select an Account...
Navigation
Alerts
Malware > Malicious Scripts
Live Dashboard
Help
Signatures
Users
Notifications

- Phishing
  - Copied Pages [2239]
  - Phishing Users [177]
  - Phishing Email [0]
- Malware
  - Malicious Scripts [87]
  - Mobile [169]
  - Infected Users [142]
- Social Media Monitoring
  - Links [0]
  - Photos [0]
  - Videos [0]
  - Users [0]
  - Bad Words [0]
  - Similar Pages [1]
  - Groups [0]
- App Store Monitoring
  - All Apps [7980]
  - Android [698]
  - iPhone [4203]
  - BlackBerry [0]
  - Windows Mobile [1561]
  - Symbian [356]
  - Opera Apps [1037]
  - Cydia Repositories [0]
  - Installous [0]
  - Facebook Apps [125]
- Logs
  - Logs [659]
- Defacement
  - Websites [4]

□ Hide Empty User Names From: Until: Severity: To: Status: Text: Clear Search

□	User Name	Alert URL	Alert Type	Host	Status	Severity	Date
☑		http:/[redacted]	Targeted Script Injection	[redacted]	Open	🟥🟥🟥🟥□	Wed 9:34 pm
□		https://[redacted]	Malicious Scripts	[redacted]	New	🟨🟨□□□	Wed 9:19 pm
□		http:/[redacted]	Targeted Script Injection	[redacted]	Open	🟥🟥🟥🟥□	Wed 8:37 pm
□		http://[redacted]	Malicious Scripts	[redacted]	New	🟨🟨□□□	2014/08/07 8:59 pm
□		http:/[redacted]	Malicious Scripts	[redacted]	New	🟨🟨□□□	2014/08/07 8:32 pm
□		http:/[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:32 pm
□		http:/[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:31 pm
□		http:/[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:26 pm
□		http:/[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:19 pm
□		http://[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:14 pm
□		http:/[redacted]		[redacted]	New	🟨🟨□□□	2014/08/07 8:13 pm
□		http://[redacted]			New	🟨🟨□□□	2014/08/07 8:08 pm
□		http://[redacted]			New	🟨🟨□□□	2014/08/07 8:08 pm
□		http:[redacted]			New	🟨🟨□□□	2014/08/07 8:08 pm
□		http:/[redacted]			New	🟨🟨□□□	2014/08/07 8:07 pm

Page 1 of 4 Displaying alerts 1 - 25 of 8

Sep 10, 2014, 9:34 pm

Targeted Script Injection

Alert URL: [redacted]

Alert Status: Open
Alert Date: Sep 10, 2014, 9:34 pm
Alert Severity: 91%
Alert ID: [redacted]

Additional Data:

Query: jtdb=1&j=http://[redacted]
User agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebK[redacted]HTML, like Gecko) Chrome/[redacted]fari/5[redacted]
Language: en-US,en;q=0.8
Client ip: [redacted]
Proxy ip: [redacted]
Alert domain: [redacted]
Tm: 2014-09-10 18:34:01
Alert details: [redacted]often a path for malware dropzones
Alert type: Targeted Script Injection

Figure 1: The Web Fraud dashboard allows users to monitor attacks targeting their organization in real time.

F5 WebSafe and MobileSafe signature tuning

F5 helps ensure that you get the most from your investment in anti-fraud services. By providing regular checks and updates to the anti-fraud, anti-malware, and anti-phishing components in F5 WebSafe and MobileSafe, the SOC ensures the effectiveness of detection and protection methods used against known financial malware—automatically strengthening fraud defense against ever changing threats.

Anti-phishing and malware monitoring and analysis

The F5 SOC provides ongoing, real-time expert monitoring and analysis of financial malware and any developing phishing sites detected by F5 WebSafe and MobileSafe or third parties. F5 teams of expert researchers continuously monitor these threat types to give insight into the proliferation of malicious software use as well as phishing attacks aimed at a specific bank or group of banking institutions, their customers, or a region or country. The F5 SOC also publishes the results of a detailed analysis that employs a combination of static and dynamic malware analysis methods to understand the full scope of malware operations, including:

- How the malware was installed and runs.
- How it behaves when executed.
- Who it communicates to and what information is shared.
- What components are installed and how they operate.

With monitoring and analysis services, the F5 SOC helps to improve defenses by protecting financial institutions and their customers against online identity theft, illegal money transfer, persistent threats, and account take overs.

Malicious site/drop zone analysis

F5 identifies and analyzes malicious command and control centers and servers that financial malware communicates with to upload stolen credentials, account information, and more for criminals to retrieve. This information enables organizations to take effective steps toward shutting down malicious services and stopping cyber attacks.

Attack assessments

To help customers understand the full scope of a financial malware attack, F5 provides detailed assessment reports that build from anti-phishing or malware analysis. These reports provide information that effectively characterizes an overall fraud attack on a specified banking URL in terms of origin(s), attack duration, number of customers affected, URLs targeted, details on suspicious transactions, attack type, and other pertinent information. Attack assessments are provided exclusively to affected customers, and any information identifying individual F5 customers remains confidential.

Malicious site shutdown

F5 provides the industry's most rapid and effective malicious site shutdown service. Once a malicious site has been identified, the experienced staff at F5 works around the clock to shut down services in minimal hours and protect an organization's reputation.[1] Shutdown services include drop zone analysis with post-service reports that provide details characterizing the drop zone. F5 also leads efforts to engage with third parties, ISPs, hosting providers, domain registrars, agencies, and law enforcement around the world to track down hosting servers and shut down malicious sites quickly.

[1] The speed at which malicious sites are shutdown may vary and is dependent upon customer involvement and responsiveness. Contact your F5 sales rep or F5 Security Operations Center specialist for complete details.

Ongoing Research and Analysis Reporting

F5 constantly monitors the fraud threat landscape, and analyzes risks and trends that threaten online financial institutions. The F5 SOC receives ongoing updates from the F5 global web fraud and security customer base, as well as from reputable information outlets and other sources around the world. F5 then passes this information on to web fraud service customers.

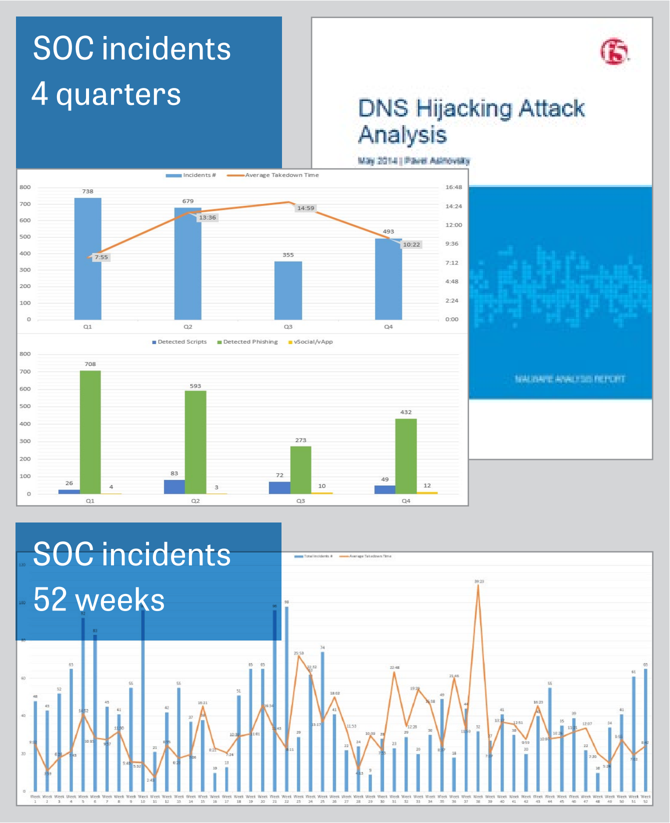


Figure 2: The F5 Security Operations Center provides a wide range of research and reports.

SOC reports reflect key research findings and highlight current and significant trends in the field. This ensures that customers are always aware of the latest fraud activities and patterns while providing insight into the potential impact threats may have on businesses. F5 also publishes quarterly and annual analytical reports and works with clients to produce customized reports based on knowledge of their business.

Support Based on Client Needs

F5 offers assigned Service Delivery Managers (SDMs) who maintain intimate knowledge of your business security services and exposure to online fraud risk. The security SDM works with individual clients and the SOC to more effectively assist in combating fraud and mitigating security risks. SDMs helps ensure your business has the right information on specific fraudulent incidents, malware discoveries, and other threats.

In addition to helping resolve immediate issues, SDMs provide proactive services, such as regular status and quarterly review meetings, to help organizations improve operations and plan for future security needs. SDMs are available during normal business hours to answer questions regarding threats and incidents, provide advice on response planning, and drive escalations to close.

More Information

To learn more about the F5 Security Operations Center and to view related published reports visit f5.com.

Web Page

F5 Security Operations Center

DevCentral

F5 Security Operations Center Report

Datasheet

F5 WebSafe and F5 MobileSafe

Reports and Analysis

Malware Summary Report: Neverquest
Neverquest Malware Analysis
Cridex Cross-device Online Banking Trojan