SOURCEfire®

Attack Risk Report

Prepared for Fake Example Inc

Wednesday 23 January 2013

This is an example report. All data contained herein is fake

Prepared By Joe Smith, AwesomeSecurity

Contact: fake@awesomesecurity.com

I. EXECUTIVE SUMMARY

Sourcefire has determined that Fake Example Inc is at a High risk due to the observation of attacks on the newtork targetting hosts that may be vulnerable. These attacks and hosts require further investigation to help lower the risk.

Assessment Period: Wed Jan 9 13:19:59 2013 to Wed Jan 23 13:19:59 2013

Total Attacks	Relevant Attacks	Hosts Targeted
13,377 	134 	19 

Irrelevant Attacks	Events Requiring Attention	Compromised Devices
99% 	1% 	25 

(A summary of the assessment results starts on page 3)

RELEVANT ATTACKS CARRY THE FOLLOWING RISKS

RISK CLASSIFICATION	NUMBER OF EVENTS
A Network Trojan was Detected	1,302
Attempted Denial of Service	1,245
Attempted Administrator Privilege Gain	1,051

Sourcefire recommends that Fake Example Inc deploy Sourcefire FirePOWER Appliances to:

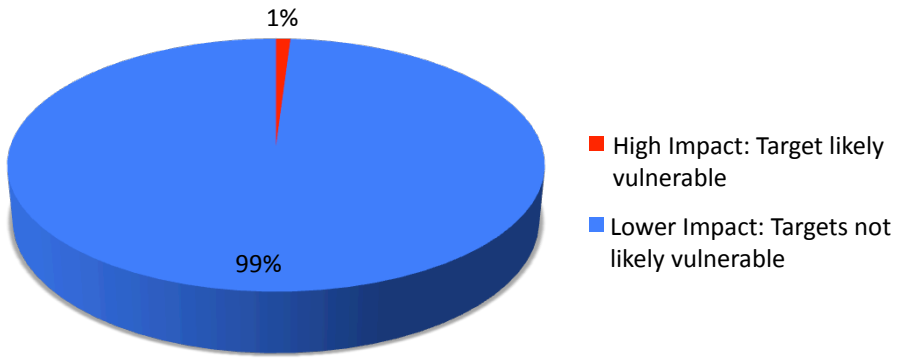
1. **Establish continual visibility into its network attack risks**
2. **Implement automated protections in order to mitigate this risk going forward**

SOURCEfire

II. ASSESSMENT RESULTS

IDENTIFYING CRITICAL ATTACKS USING IMPACT ANALYSIS

Of the 13377 total attacks made on your network, 134 (1%) of them were considered high impact. That means that they targeted machines that were likely vulnerable to these attacks. These events are the most critical to investigate, and Sourcefire automatically identifies them for you. Sourcefire identifies high impact events automatically by correlating attacks with target risk, which is determined by passively profiling your network devices and their vulnerabilities in real time. This saves time and money over traditional solutions, which require you to qualify all events manually or import scan data from other systems.If a staff member's time is worth $75 USD per hour and each attack takes 20 seconds to qualify, then each attack costs $0.42 USD to manually qualify. The difference in qualification time and cost between Sourcefire and traditional solutions is substantial.



ATTACKS TO QUALIFY / YEAR	COST TO QUALIFY	COST TO QUALIFY ALL ATTACKS
348,940 estimated total attacks	0.42	146,555
3,494 estimated high impact attacks	0.42	1,467

	COST SAVINGS
Year #1	**$145,088**
Year #5	**$725,440**

SOURCEfire

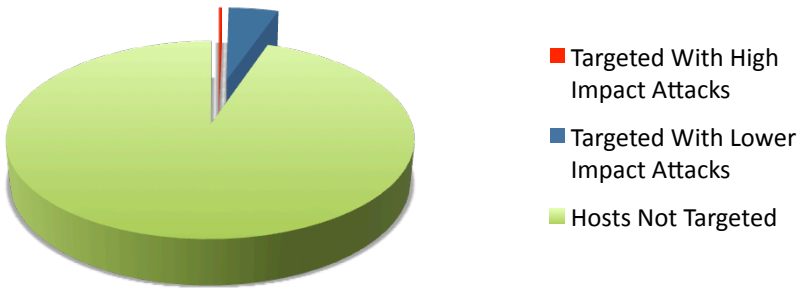
HIGH IMPACT ATTACKS

The following attacks are very important to investigate because they directly target machines that have been identified as potentially vulnerable. The target machine's operating system version, running services, and potential vulnerabilities all match what the threat is designed to attack.

EVENT TYPE	DETAILS	APPLICATION	POTENTIALLY VULNERABLE HOSTS
A Network Trojan was Detected	MALWARE-CNC Win.Trojan.ZeroAccess outbound communication	ActiveSync	10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4
Attempted Administrator Privilege Gain	BROWSER-IE Microsoft Internet Explorer getElementById object corruption	HTTP	192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4
Attempted Administrator Privilege Gain	OS-WINDOWS DCERPC Messenger Service buffer overflow attempt	HTTP	172.16.12.3, 172.16.43.1, 10.0.3.4, 10.45.1.4
A Network Trojan was Detected	RPC sadmind query with root credentials attempt UDP	HTTP	192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4
Attempted Administrator Privilege Gain	BLACKLIST User-Agent known malicious user-agent string AHTTPConnection	HTTP	10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4

HOSTS AT HIGH RISK

0.3% of your hosts have been targeted with high impact attacks during the assessment period. They are at high risk of infection. The attacks should be investigated and the machines assessed to ensure that proper controls are in place. An additional 4.9% of the machines discovered on your network were targeted with some form of attack.



SOURCEfire

HOSTS ALREADY COMPROMISED

Special attention should be paid to computers already compromised by malware as they are likely to be exfiltrating information from your private systems. Systems that fall into this category likely have had malware residing on them for some time already and the initial infection has been missed by existing security protections.

SAMPLE LIST OF COMPROMISED DEVICES	
10.88.4.5	10.0.4.5
10.86.12.5	192.168.5.1
192.168.33.1	10.45.66.1
10.34.5.1	
10.88.1.5	

TOTAL HOSTS CONNCTED TO BOTNET C&C SERVERS
25

The systems listed above are exhibiting signs of compromise as they are connecting outbound to known Command and Control (C&C) servers tracked by the Sourcefire Vulnerability Research Team (VRT). You should take action to remediate or restore these systems.

AUTOMATING THE TUNING EFFORT

During the assessment period the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A New Operating System was found	93,181
A new host is added to the network	7,060
A device starts using a new transport protocol	181,284
A device starts using a new network protocol	124,153

As network changes are made, Sourcefire solutions automatically adjust policy so that new operating systems, hosts and protocols are protected. Sourcefire automates the tuning process by monitoring networks in real time and observing changes, and then making appropriate policy changes as a result. For example, if Windows 2000 hosts running IIS appear on a network, Sourcefire ensures that rules protecting against Windows 2000 and IIS vulnerabilities, and not irrelevant rules that may cause false positives, protect these hosts.

SOURCEfire®

APPLICATIONS ASSOCIATED WITH ATTACKS

The following applications have been identified as associated with attacks. You should identify applications in this list that have low business relevance and evaluate whether it would be helpful to control them on your network.

APPS ASSOCIATED WITH HIGH IMPACT EVENTS	COUNT
ActiveSync client	134
WebEx client	91
Web browser	23
Mobile Safari	9
DNS client	1

APPS ASSOCIATED WITH LOW IMPACT EVENTS	COUNT
ActiveSync client	18,084
Web browser	232
WebEx client	222
Chrome	30
DNS client	20

TOP ATTACKERS AND TARGETS

The top attackers and target machines observed in the attack attempts on your network are listed below. For high impact attacks in particular, you should ensure that targets are well protected from potential attackers by patching these machines and blocking potentially malicious traffic.

	ATTACKERS	ATTACKS	TARGETS	ATTACKS
HIGH IMPACT EVENTS	10.2.5.1	81	10.33.55.11	67
	183.51.1	21	10.65.22.45	16
	172.15.6.1	32	10.88.44.22	9
	192.168.44.1	14	10.9.3.5	3
	192.168.62.4	9	10.5.1.3	1
LOW IMPACT EVENTS	10.51.62.3	33	192.168.62.1	119
	10.72.23.51	19	10.76.33.6	112
	255.235.61.3	18	10.46.26.4	12
	10.35.61.3	16	10.82.63.57	7
	192.168.76.64	12	10.57.15.6	4

SOURCEfire

IPv6 ATTACKS AND TRAFFIC

IPv6 traffic is a potential avenue for attacks that is often left unprotected by organizations. Network security is often thought of strictly from an IPv4 perspective, yet hosts may communicate internally and even externally to an organization over IPv6, exposing them to attack risks. The following communications were observed over IPv6 during the assessment period.

HOSTS USING IPv6 IN YOUR NETWORK (MONITORED)	ATTACKS SEEN OVER IPv6
187	**786**

III. BUSINESS RISK OF ATTACKS

BUSINESS RISK OF INTRUSION ATTEMPTS

Different types of attacks were detected on the Fake Example Inc network, each introducing different business risks. Here are the most common attack types observed along with the risks each introduces.

ATTACK CLASSIFICATION	NUMBER OF EVENTS	RISK ASSOCIATED WITH THE ATTACK
Potential Corporate Policy Violation	14	**Information Theft:** These events indicate usage of apps and protocols in ways that may be prohibited by organizational policy.
A Network Trojan was Detected	134	**Infrastructure Damage, Information Theft:** A Trojan horse is a program that appears to be benign to an end user but is in fact malicious. It can be used to steal information or cause damage.
Attempted Denial of Service	4	**System Degradation, Denial of Service:** Denial-of-service attacks attack the reliability of your network infrastructure, causing service to be denied to legitimate users.
Attempted Administrator/User Privilege Gain	19	**Information Theft, Infrastructure Damage**: Users on network machines who gain privileges illicitly may be able to steal information, control machines

SOURCEfire®

IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, critical attacks are taking place and placing your organization at risk. New countermeasures and security controls are required to mitigate the risk.

Sourcefire recommends deployment of network-based protections via FirePOWER NGIPS Appliances to complement existing protections. These will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Real-Time Contextual Awareness	Profile hosts, applications, users, and network infrastructure in real time. Assess potential vulnerabilities and identify network changes.
Automatic Impact Assessment	Determine the risk of any attack to your business in real time in order to optimize response to it.
Automatic Policy Tuning	Automatically tune IPS protections in response to changes in your network composition.
Association of Users with Security and Compliance Events	Associate users with activity on the network, including attacks and application usage, through integration with Active Directory servers.
Collective Intelligence	Get rapid detection and insight into emerging threats so that defenses stay effective
Virtual Protection	Protect VM-to-VM communications the same as physical networks

In addition, Sourcefire offers optional Advanced Malware Protection for networks and hosts, and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Sourcefire representative or reseller for more information.

SOURCEfire®

ABOUT SOURCEFIRE

Sourcefire Inc. (Nasdaq: FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize network security risks. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire provides customers with Agile Security TM that is as dynamic as the real world it protects and the attackers against which it defends.

Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with numerous patents, world- class research, and award winning technology. Today the name Sourcefire has grown synonymous with innovation, security intelligence and agile end toned security protection.

CONTACT US

Want to learn more about getting this information on your network? Go to http://info.sourcefire.com and request a live demo.

Agile Security