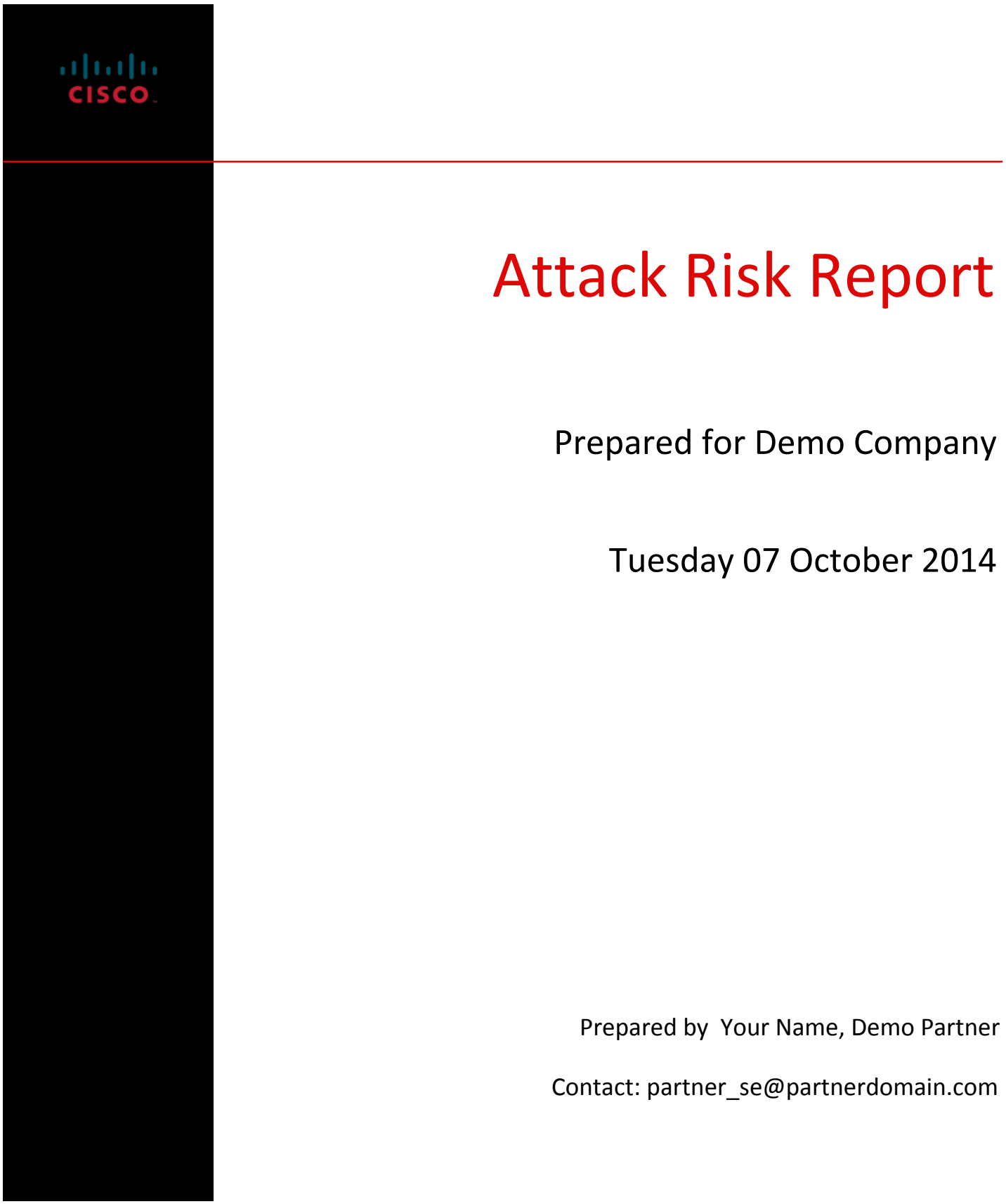


Attack Risk Report

Prepared for Demo Company

Tuesday 07 October 2014

Prepared by Your Name, Demo Partner

Contact: partner_se@partnerdomain.com

I. EXECUTIVE SUMMARY

Cisco has determined that Demo Company 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 Jul 9 09:12:27 2014 to Tue Oct 7 09:12:27 2014

Total Attacks	Relevant Attacks	Hosts Targeted
656 	10 	1 

Irrelevant Attacks	Events Requiring Attention	Hosts Connected to CnC Servers
98.5% 	1.5% 	2 

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

RELEVANT ATTACKS CARRY THE FOLLOWING RISKS

RISK CLASSIFICATION	NUMBER OF EVENTS
Attempted User Privilege Gain	10

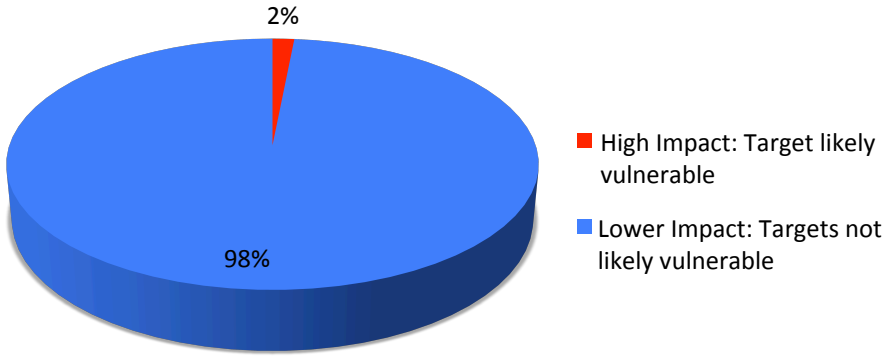
Sourcefire recommends that Demo Company deploy Sourcefire FirePOWER Appliances to:

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

II. ASSESSMENT RESULTS

IDENTIFYING CRITICAL ATTACKS USING IMPACT ANALYSIS

Of the 656 total attacks made on your network, 10 (1.5%) 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 Cisco automatically identifies them for you. Cisco 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 10 seconds to qualify, then each attack costs $0.21 USD to manually qualify. The difference in qualification time and cost between Cisco and traditional solutions is substantial.



ATTACKS TO QUALIFY / YEAR	COST TO QUALIFY	COST TO QUALIFY ALL ATTACKS
2,555 estimated total attacks	0.21	537
41 estimated high impact attacks	0.21	9

	COST SAVINGS
Year #1	**$528**
Year #5	**$2,640**

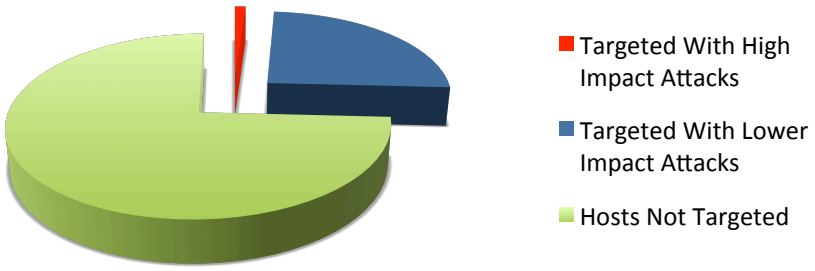
HIGH IMPACT ATTACKS

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
Attempted User Privilege Gain	BROWSER-IE Microsoft Internet Explorer malformed span/div html document heap corruption	HTTP	1.1.1.1, 2.2.2.2
		n/a	
		n/a	
		n/a	
		n/a	

HOSTS AT HIGH RISK

1.1% 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 24.7% of the machines discovered on your network were targeted with some form of attack.



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
1.1.1.1
1.1.1.2

TOTAL HOSTS CONNCTED TO BOTNET C&C SERVERS
2

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 Cisco 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	431
A new host is added to the network	438
A device starts using a new transport protocol	438
A device starts using a new network protocol	538

As network changes are made, Cisco solutions automatically adjust policy so that new operating systems, hosts and protocols are protected. Cisco 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, Cisco ensures that rules protecting against Windows 2000 and IIS vulnerabilities, and not irrelevant rules that may cause false positives, protect these hosts.

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
Chrome	1

APPS ASSOCIATED WITH LOW IMPACT EVENTS	COUNT
OpenSSH	494
Mobile Safari	140
Chrome	7
MobileAsset	6
DNS client	5

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	1.1.1.1	4	1.1.1.1	4
	2.2.2.2	1	1.1.1.2	1
LOWER IMPACT EVENTS	1.1.1.1	382	2.2.2.1	389
	1.1.1.2	118	2.2.2.2	134
	1.1.1.3	56	2.2.2.3	111
	1.1.1.4	51	2.2.2.4	64
	1.1.1.5	45	2.2.2.5	31

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
46	**656**

III. BUSINESS RISK OF ATTACKS

BUSINESS RISK OF INTRUSION ATTEMPTS

Different types of attacks were detected on the Demo Company 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	0	Information Theft: These events indicate usage of apps and protocols in ways that may be prohibited by organizational policy
A Network Trojan was Detected	94	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	0	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	13,868	Information Theft, Infrastructure Damage: Users on network machines who gain privileges illicitly may be able to steal information, control machines

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.

Cisco 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, Cisco 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 Cisco representative or reseller for more information.

ABOUT CISCO

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It's more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For nearly three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

Cisco delivers intelligent cybersecurity for the real world.

CONTACT US

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