I. EXECUTIVE SUMMARY

Cisco has determined that [redacted] 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: Fri Apr 17 09:14:35 2015 to Fri May 1 09:14:35 2015

Total Attacks	Relevant Attacks	Hosts Targeted
62,992	1,075	41

Irrelevant Attacks	Events Requiring Attention	Hosts Connected to CnC Servers
98.3%	1.7%	42

(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	1,072
Attempted User Privilege Gain	1
Misc Activity	2

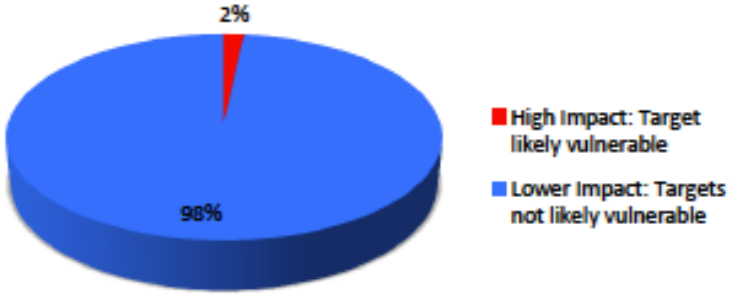
Sourcefire recommends that [redacted] deploy Sourcefire FirePOWER Appliances to:

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 62992 total attacks made on your network, 1075 (1.7%) 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
1,642,135 estimated total attacks	0.21	344,848
28,027 estimated high impact attacks	0.21	5,886

	COST SAVINGS
Year #1	$338,962
Year #5	$1,694,810

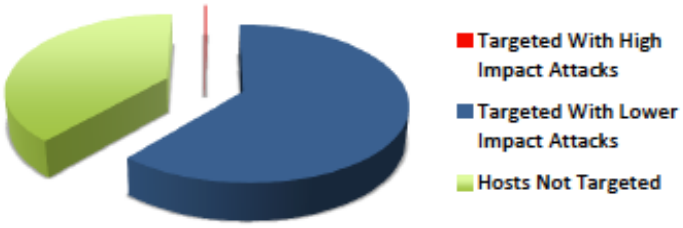
HIGH IMPACT ATTACKS

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.Mudrop variant outbound connection	HTTP	8.34.112.66, 70.186.131.116
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain counter.yadro.ru	DNS	8.8.8.8, 10.188.1.4, 10.188.1.6, 88.212.196.87,
A Network Trojan was Detected	APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com	DNS	10.188.1.4, 10.188.1.6
A Network Trojan was Detected	APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn	DNS	10.188.1.4, 10.188.1.6, 194.168.4.100, 194.168.8.100
A Network Trojan was Detected	BLACKLIST DNS request for known malware domain zstats.cc	Kugou	10.188.1.4, 10.188.1.6

HOSTS AT HIGH RISK

0.2% 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 61.1% of the machines discovered on your network were targeted with some form of attack.



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
0	62,992

III. BUSINESS RISK OF ATTACKS

BUSINESS RISK OF INTRUSION ATTEMPTS

Different types of attacks were detected on the Warwickshire LEA 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	27,095	Information Theft: These events indicate usage of apps and protocols in ways that may be prohibited by organizational policy
A Network Trojan was Detected	1,208	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
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	0	Information Theft, Infrastructure Damage: Users on network machines who gain privileges illicitly may be able to steal information, control machines