SOURCEfire®

# Network 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 use of applications that are potentially dangerous to the enterprise yet have low business relevance. These applications may leave your network vulnerable to attack, carry malware, or waste bandwidth.

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

| Risky Apps | Risky Users | High Bandwidth Apps |
|---|---|---|
| 44 | * | 78 |

* AD Integration disabled

| Encrypted Apps | Evasive Apps | Dangerous Web Browsers |
|---|---|---|
| 51 | 12 | 51 |

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

## YOUR NETWORK PROFILE

| 24 | 579 | 1146 | 8 |
|---|---|---|---|
| Operating Systems | Mobile Devices | Applications In Use | File types transferred |

## RECOMMENDATIONS

Sourcefire recommends Fake Example Inc deploy Sourcefire FirePOWER Appliances (NGIPS/NGFW) with App Control and URL Filtering to:

1. Reduce your application attack surface
2. Granularly control applications, bandwidth, URL access and acceptable use policies
3. Get visibility into network risks and usage, including mobile devices and BYOD risk

SOURCEfire

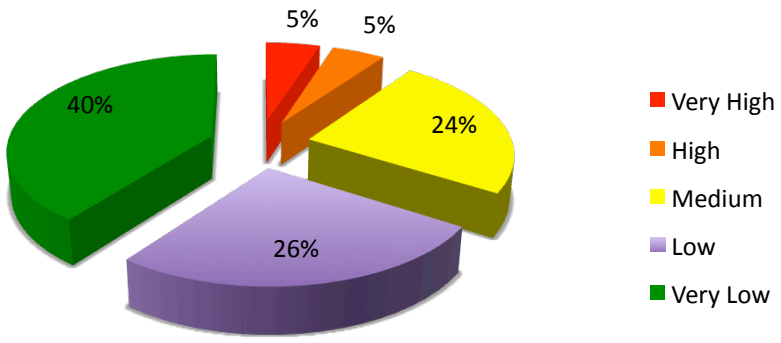
# II. APPLICATION RISK

## APPLICATIONS WITH HIGH RISK AND LOW BUSINESS RELEVANCE

Some applications carry high risk because they can be vectors for malware into the organization, possess recent vulnerabilities, use substantial network resources, or hide the activities of attackers. Other applications have low business relevance: they are not relevant to the activities of a typical organization. When an application has high risk and low business relevance, it is a good candidate for application control to reduce your application risk. You should investigate these applications to determine whether they are important to control.

| APPLICATION | TIMES ACCESSED | APPLICATION RISK (1-5) | PRODUCTIVITY RATING (1-5) | DATA TRANSFERRED (MBYTES) |
|---|---|---|---|---|
| BitTorrent | 187,472 | Very High | Very Low | 19,312.57 |
| daytime | 179,559 | Very High | Very Low | 67.45 |
| GIOP | 37,188 | Very High | Very Low | 652.50 |
| Movie2k.to | 2,348 | Very High | Very Low | 1,373.16 |
| daytime | 1,530 | Very High | Very Low | 35.50 |

**SUMMARY OF ALL NETWORK CONNECTIONS BY APPLICATION RISK**



## HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

| APPLICATION | TIMES ACCESSED | APPLICATION RISK (1-5) | PRODUCTIVITY RATING (1-5) | DATA TRANSFERRED (MBYTES) |
|---|---|---|---|---|
| YouTube | 766,305 | High | Very Low | 450,134.28 |
| Netflix stream | 79,042 | Very Low | Very Low | 306,129.46 |
| MP4 | 83,085 | Very Low | Medium | 187,873.84 |
| Netflix | 287,569 | Medium | Very Low | 147,819.52 |
| Flash Video | 7,747 | Medium | High | 91,165.65 |

## ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Sourcefire SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

| APPLICATION | TIMES ACCESSED | APPLICATION RISK (1-5) | PRODUCTIVITY RATING (1-5) | DATA TRANSFERRED (MBYTES) |
|---|---|---|---|---|
| Facebook | 4,119,315 | Very High | Low | 100,135.80 |
| Gmail | 254,150 | Low | Medium | 18,719.20 |
| Amazon | 102,904 | Very Low | Low | 3,138.58 |
| SSL | 102,904 | Medium | Medium | 3,138.58 |
| BitTorrent | 187,472 | Very High | Very Low | 19,312.57 |

SOURCEfire

## EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

| APPLICATION | TIMES ACCESSED | APPLICATION RISK (1-5) | PRODUCTIVITY RATING (1-5) | DATA TRANSFERRED (MBYTES) |
|---|---|---|---|---|
| BitTorrent | 5,874,514 | Very High | Very Low | 85,269.36 |
| Xunlei | 19,830 | Very High | Very Low | 332.95 |
| Privax | 43 | Very High | Very Low | 0.86 |
| Skype | 18,234 | Very High | Medium | 840.46 |
| Ares | 1,855 | High | Very Low | 3.59 |

## OTHER APPLICATIONS OF INTEREST

Other applications were observed that may be of interest and possibly candidates for control. Users may use anonymizers and proxies to bypass your network security or cloak their identities. Gaming applications may be distractions to productivity and use excessive bandwidth. Peer-to peer applications are often malware vectors. And remote administration applications may allow malicious users to control machines in your environment.

**Anonymizers and Proxies (accesses):**
*Squid(336) , SOCKS(178) , Avocent(42) , TOR(6)*

**Games and Recreation (accesses):**
*Facebook(2202) , Instagram(1468), Facebook message(1468), Facebook Chat(1462), Facebook Apps(1204), Flixster(896),*

**Peer-to-Peer and Sharing (accesses):**
*Skype Tunneling(1057), Skype p2p(847), eDonkey(777), IceShare(734), Windows Live(336), Instagram(336), MSN(336),*

**Remote Administration and Storage (accesses):**
*Sun RPC(723) , WebEx(368) , HTTPS(336) , iCloud(336) , Instagram(336) , HTTP(336) , Wordpress(336) , Dropbox(327) , LogMein(304)*

SOURCEfire

## DANGEROUS WEB BROWSER VERSIONS

A profile of your network revealed the following old web browsers in use. Outdated web browsers are a major vector for network malware and it is important to update them (or encourage users to). These browsers often have unpatched vulnerabilities or carry other risks.

| BROWSER | VERSION | NUMBER OF HOSTS |
|---|---|---|
| Internet Explorer | 4, 4.01, 5, 5.5, 5.01 | 34 |
| Chrome | 13, 12, 11 | 36 |
| Safari | 3.1.1, 3.2, 4 | 79 |
| Firefox | 12, 13.1, 12, 14, 15 | 18 |

## RISKY WEB BROWSING

The following web communications were identified that correspond to risky activity. Malware sites, open proxies and anonymizers, keyloggers, phishing sites, and spam sources are all Web activities that can put your networks at risk. It is wise to evaluate the use of URL filtering technologies to detect and control communications to risky sites.

| URL CATEGORY | CONNECTIONS | BLOCKED | DATA INBOUND (BYTES) | DATA OUTBOUND (BYTES) |
|---|---|---|---|---|
| SPAM URLs | 24,159 | | 1,502,002,844 | 198,660,632 |
| Spyware and Adware | 3,809 | | 39,808,214 | 8,688,192 |
| Proxy Avoid and Anonymizers | 865 | | 8,130,028 | 3,647,207 |
| Phishing and Other Frauds | 2,497 | | 257,774,021 | 20,581,294 |
| Malware Sites | 55,445 | | 2,634,973,064 | 262,957,415 |
| Hacking | 510 | | 15,031,917 | 1,806,426 |
| Peer to Peer | 15,586 | | 405,120,416 | 51,222,150 |
| Social Network | 4,758,129 | | 197,000,000,000 | 35,361,558,212 |
| Adult and Pornography | 1,768,776 | | 84,901,911,757 | 9,358,080,762 |
| | | | | |

## THE APPLICATIONS ON YOUR NETWORK

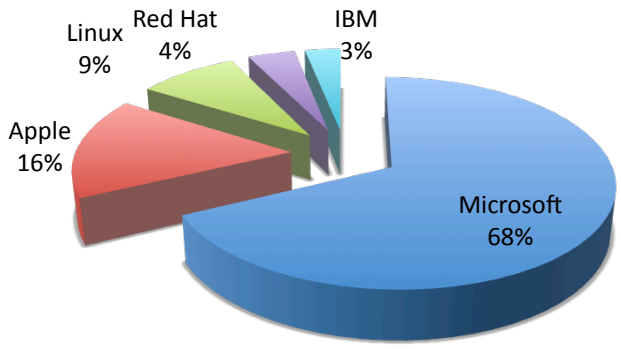
This is a list of the top applications discovered in use on your network. Three types of applications are identified and listed here: client applications (including web browsers), web applications (which run over HTTP), and server applications (for example, web servers). Full visibility over all application types enables you to get better perspective on how your networks are currently utilized.

| CLIENT APPLICATIONS | WEB APPLICATIONS | SERVER APPLICATIONS |
|---|---|---|
| Client applications include web browsers and other desktop applications that access the network | Web applications are carried over Web-related protocols like HTTP and HTTPS. Many Web applications operate on port 80. | Server applications include web servers such as IIS and Apache. |
| **Total: 312** | **Total: 629** | **Total: 178** |
| TeamViewer client, MMS, Facebook, Skype (Mac), Manolito client… | The Pirate Bay, ICQ2Go, TeamViewer, Movie2k.to, BitTorrent… | MagicJack, TFTP, eDonkey, MMS, IMAP… |

# III. ASSET PROFILE

## THE OPERATING SYSTEMS ON YOUR NETWORK

The operating systems below were observed on your network. You should identify any operating systems that fall outside your IT policy and investigate them further as to whether they should be permitted.



SOURCEfire

## THE MOBILE DEVICES ON YOUR NETWORK

The following mobile devices were profiled on your network. Mobile devices may be vulnerable, especially older or jailbroken versions. It is important to be aware of how mobile devices are used and set appropriate security policies.

| DEVICE TYPE | VERSION | COUNT |
|---|---|---|
| Apple | iOS 5.0 | 238 |
| Google | Android 4.0.4 | 178 |
| Google | 4.0.4 | 155 |
| Google | 4.0.3 | 144 |
| Apple | iOS 5.1.1 | 135 |

## THE FILES TRAVERSING YOUR NETWORK

| | FILE CATEGORY | FILE TYPE | COUNT | PROTOCOL |
|---|---|---|---|---|
| DOWNLOADS | Multimedia | SWF | 220,127 | HTTP |
| | PDF files | PDF | 4,811 | HTTP |
| | Archive | JAR | 4,742 | HTTP |
| | Executables | MSEXE | 3,121 | HTTP |
| | Office Documents | MSOLE2 | 363 | HTTP |
| UPLOADS | Executables | MSEXE | 2 | HTTP |
| | PDF files | PDF | 265 | HTTP |
| | Office Documents | MSOLE2 | 72 | HTTP |
| | | | | |
| | | | | |
| MISC | PDF files | PDF | 265 | POP3 |
| | Office Documents | MSOLE2 | 72 | POP3 |
| | Office Documents | NEW_OFFICE | 62 | POP3 |
| | Office Documents | XLW | 9 | POP3 |
| | | | | |

SOURCEfire

# IV. RECOMMENDATIONS

Despite existing protections, your organization's application usage exposes it to added risks. This assessment, which contains a profile of your network, has identified risky assets. New countermeasures and security controls are required to mitigate the risks to these assets.

Sourcefire recommends that FirePOWER Appliances with Application Control and URL Filtering are depoyed to:

**1) Establish continuous network visibility into its application and asset risk.**
**2) Augment its existing controls in order to mitigate this risk**

## 1) ESTABLISH CONTINUOUS NETWORK VISIBILITY INTO APPLICATION RISK

Existing security infrastructure provides inadequate protection against application and asset risks. Sourcefire recommends deployment of network-based protections via FirePOWER Appliances (NGIPS/ NGFW). These will provide the following new capabilities and benefits to augment your network visibility:

| NEW CAPABILITY | BENEFIT |
|---|---|
| Network Map | Profiles hosts on the network, including network infrastructure, desktops, servers, mobile devices, virtual machines, and many others. |
| Application Awareness | Identifies over 1,000 applications, including client applications that run on desktops, server applications such as Web servers, and Web applications carried over HTTP. Profiles application actions, like the ability to send email or chat using a Web mail application. |
| Mobile Awareness | identifies and profiles mobile devices, including iOS, Android, Amazon, Blackberry, and other mobile device types. Identifies jailbroken devices. |
| Real-time Contextual Awareness | Profiles hosts and identifies communications that are of unusual bandwidth or hosts that are running inappropriate applications for the environment. |

## 2) AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk applications pose. These measures may entail reduction of the application threat surface and blocking risky URLs. Sourcefire recommends deployment of network-based protections via FirePOWER Appliances with Application Control and URL Filtering. These provide the following new capabilities and benefits:

| NEW CAPABILITY | BENEFIT |
|---|---|
| Granular Application Control | Reduce potential area of attack through granular control of thousands of applications. Filter and enforce usage policy on millions of URLs. |
| URL Filtering | Control on a database of millions of URLs, by risk or productivity characteristics |
| Virtual Protection | Protect VM-to-VM communications the same as physical network |

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

The operating systems below were observed on your network. You should identify any operating systems that fall outside your IT policy and investigate them further as to whether they should be permitted.

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.