



Cloud

Solutions



Cybersecurity



Industries



Why

Neovera



F

Cybersecurity Insight

# Neovera Threat Intelligence Short Report – December 31st, 2015

31 DEC

## Emerging Threat – Juniper ScreenOS Backdoor

An [advisory](#) has been issued that unauthorized code in the ScreenOS software that powers Juniper's NetScreen firewalls has been discovered. There are two distinct issues: a backdoor in the VPN implementation that allows a passive eavesdropper to decrypt traffic and a second backdoor that allows an attacker to bypass authentication in the SSH and Telnet daemons. Exploitation of these vulnerabilities can lead to complete compromise of the affected device.

We added IDS signatures and correlation rules to detect

Connect with  
Neovera  
Experts



We are a small, yet powerful consulting partner where you work directly with our executive

the relevant activity:

- Reconnaissance & Probing, Backdoor, Juniper ScreenOS telnet Backdoor Default Password Attempt
- Environmental Awareness, Vulnerable software, Exposed Juniper ScreenOS

## Emerging Threat – Emissary

A [targeted attack](#) in November directed at a French Diplomat working for the French Ministry of Foreign Affairs. The attack attempts to exploit CVE-2014-6332 using a slightly modified version of the proof-of-concept (POC) code to install a Trojan called Emissary, which is related to the [Operation Lotus Blossom](#) campaign.

We added IDS signatures and a correlation rule to detect Emissary:

- System Compromise, Targeted Malware, Emissary

## New Detection Technique – BBSRAT

[BBSRAT](#) is a new tool that attacks Russian Organizations linked to [Roaming Tiger](#). It uses weaponized exploit documents and leaves Russian language decoy document files after infecting the system. The files exploit the well-known Microsoft Office vulnerability, CVE-2012-0158, to execute malicious code in order to take

leadership team - experts who have earned a pre-eminent reputation in cybersecurity solutions and managed services. Request a consultation for a customized program for your organization.

**Talk With An  
Expert**

control of the targeted systems. BBSRAT uses the same C2 domains as previously published in the “Roaming Tiger” campaign

We added IDS signatures and correlation rules to detect the following RAT activity:

- System Compromise, Malware RAT, BBSRAT
- System Compromise, Malware RAT, BBSRAT SSL Certificate

## **New Detection Technique – Remote Access Tools**

The typical attack pattern involves first an attack (exploited vulnerability) and then installation of malware. Often this last step includes a Remote Administration Toolkit (RAT) used to gain control to the compromised machine.

- System Compromise, Malware RAT, ExysRAT
- System Compromise, Malware RAT, AresRAT

## **New Detection Technique – Malware**

The following correlation rules have been added due to recent malicious activity:

- System Compromise, Hacking tool, Metasploit Meterpreter
- System Compromise, Targeted Malware, Fexel
- System Compromise, Targeted Malware, Ironhalo
- System Compromise, Targeted Malware, Elmer
- System Compromise, Backdoor, WeBaCoo Web Backdoor Detected
- System Compromise, Ransomware infection, Radamant

## Updated Detection Technique – Exploit Kits

Exploit kits are used in what are called “Drive-by Downloads.” Undetectable by normal users, these kits are embedded in websites by attackers. When a user browses to a website hosting an exploit kit, the kit attempts all known attacks to compromise the user and install malware on their machine. This approach is a common attack vector and a major source of infections for end users.

Cybercriminals constantly change the patterns they use within their code to evade detection. This week we added the following IDS signatures and updated correlation rules to enhance exploit kit detection:

- Delivery & Attack, Malicious website – Exploit Kit,

## Neutrino EK

- Exploitation & Installation, Malicious website – Exploit Kit, Angler EK

## Updated Detection Technique – Malware SSL Certificates

We have added new IDS signatures to include the list of certificates identified by [Abuse.ch](https://abuse.ch) to be associated with malware of botnet activities. The new correlation rules use this information to detect C&C communications related to several malware families, including:

- System Compromise, C&C Communication, Gootkit SSL activity
- System Compromise, C&C Communication, Gozi SSL Activity
- System Compromise, C&C Communication, Known malicious SSL certificate

## Updated Detection Technique – Tor Onion Proxy

Tor is an open network that enables anonymity and allows users to surf the Internet anonymously. Tor also provides anonymity for servers that can only be accessed through the Tor network, called hidden services. There are some websites that allow access to Tor hidden services through the Internet without being inside the Tor network.

We have created a new correlation rule that will detect when a system is accessing one of these services. Many ransomware schemes use these services to receive payments and conduct other malicious activities.

- Environmental Awareness, Anonymous channel, Tor Onion Proxy

## Updated Detection Technique – Malicious TOR .onion domain

.onion is a top level domain suffix that is used for hidden services inside the Tor network. Several families of malware are starting to use hidden services as a mechanism to communicate with a C&C server and usually use a predefined onion domain. We have updated a correlation rule that groups different IDS signatures that detect when a system is trying to resolve a malicious onion domain:

- System Compromise, Malware infection, Malicious TOR .onion domain

## Updated Detection Technique – Ransomware

Last week we added IDS signatures and updated correlation rules to detect several ransomware families:

- System Compromise, Ransomware infection, Alphacrypt

# Updated Correlation Rules

The following correlation rules have been updated due to recent malicious activity:

- Delivery & Attack, Malicious website, Phishing activity
- System Compromise, Malware RAT, Poison Ivy
- System Compromise, Malware infection, CoinMiner
- System Compromise, Malware infection, Darkleech
- System Compromise, Malware infection, Generic
- System Compromise, Targeted Malware, DeputyDog
- System Compromise, Trojan infection, Banload
- System Compromise, Trojan infection, Bitcoin Miner
- System Compromise, Trojan infection, Dorv.A
- System Compromise, Trojan infection, Jaik
- System Compromise, Trojan infection, Kelihos
- System Compromise, Trojan infection, Linux DDoS Bot
- System Compromise, Trojan infection, Winwebsec

## SHARE



[Case Studies](#)[Cloud Insight](#)[Cybersecurity Insight](#)[Live/Virtual Events](#)[Managed Services](#)[Partner Community Insight](#)[Press Releases](#)

## Get the Latest News & Insights

Follow  
Us

First Name \*





Email \*

Submit





Chicago | Washington |  
New York  
(866) 636-8372

**Cloud**

**Solutions**

**Cybersecurity**

**Solutions**

**Industries**

**Why Neovera**

**Resources**

**COMPANY**

Leadership

Careers

**DISCOVER HOW WE**

**WORK**

If you are interested in learning more about Neovera’s services, we are happy to help you.

This website uses cookies in order to provide a better user experience and functionality. By continuing to browse the site you agree to our Privacy policy.

[Ok](#) [Privacy policy](#)