

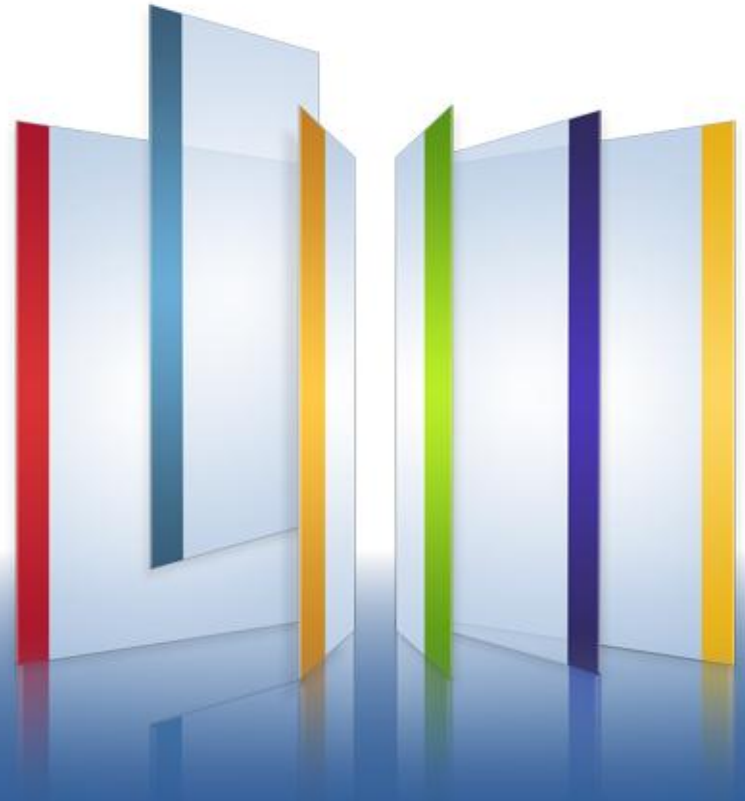


Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Threat Prevention

*from (Unified) Threat Management
to Prevention*



The Cyber War Rages On...

700%

Malware growth
between 2007-2012

82%

of organizations
experienced a **bot** attack

59%

of organizations believe they
experienced a targeted **APT** attack



¹ AV-Test March 2012 Malware stats

² Ponemon 2nd annual cost of cybercrime study August 2011

³ Verizon 2012 Data Breach Investigations Report

Check Point Multi Layered Threat Prevention



Multi Layered Threat Prevention - Firewall



**Protect against
unauthorized access**

Contain infections in network segments

Multi Layered Threat Prevention – IPS



Check Point®
SOFTWARE TECHNOLOGIES LTD.



Stop attacks exploiting vulnerabilities

**Protect against exploit of vulnerabilities in:
Word, Excel, PDF, Browsers, Operating Systems...**



softwareblades™

Multi Layered Threat Prevention – Antivirus



Block Malware Download

**Block Malware file download and
access to malware containing sites**



Antivirus Software Blade

Extended Protection Using ThreatCloud™

**Stop Incoming
Malware
Attacks**

**Protect with 300x
More Signatures
with ThreatCloud**



**Prevent
Access to
Malicious Sites**

**Over 300,000
Malicious Sites**



Unified View

**See the Big
Malware Picture**



Stop Incoming Malicious Files

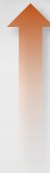


300x More Signatures than Previous Versions

ThreatCloud™



Unique file
identifier



File is
malicious



**50,000 New Malware
Signatures Added
to ThreatCloud™
Every Day**



Prevent Access to Malware-Infested Websites

ThreatCloud™



Site
Address



Malware
containing site



**91% of attacks
come from
malicious URLs,
making them the #1
internet threat***

* Kaspersky Monthly Malware Statistics February 2012

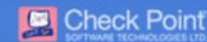
Unified View of Anti-Malware



See the BIG Malware Picture

MALWARE REPORT

Monthly Report | September 1st 2011 - September 31st 2011 | Origin - London-GW



Anti-Bot Blade:  Active Anti-Virus Blade:  Active

Generated by Check Point SmartEvent[®], on September 2nd 2011 10:35AM **1**



1290

Protected Hosts

 **70 Hosts**

Involved in Malicious Activity

 **12 (2 new)**

Detected Malwares



Top Hosts

Involved in Malicious Activity

Dan.D-LapTop **55 incidents**

John.S-Desk **34 incidents**

Jane.P-Lab **32 incidents**

Web.Server2 **21 incidents**

Web.Proxy3 **19 incidents**



Top Malwares Found

14 hosts infected in **Devastator**

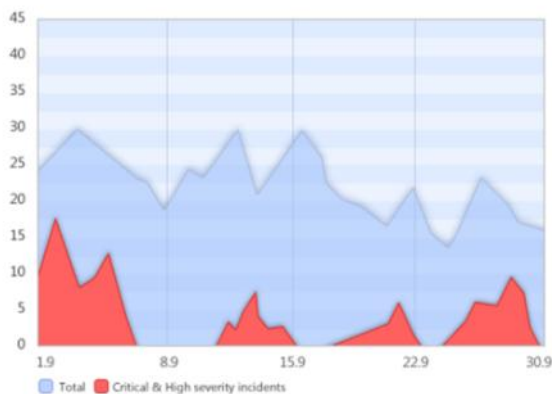
10 hosts infected in **Welchia Blaster**

15 hosts infected in **Trojan.Downloader**

5 hosts infected in **Z.bot**

5 hosts infected in **SpyEye**

Incidents in the Last Month



600

Malicious Incidents

 **400**
Prevented

 **200**
Detected

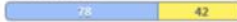

 **135MB**
Total Sent

 **20MB**
Total Received

C&C Communication / Data Leak

 **85**  -81

DDOS Attacks

 **120**  24

Self Distribution Attempts

 **180**  35

Click Fraud Hits

 **78**  -5

Outgoing Spam Mail

 **135**  90

 Prevent  Detect (Policy can be modified to prevent more or all incident types)

  In comparison to previous month



Multi Layered Threat Prevention – Anti-Bot



Discover and stop Bot Attacks

**Post infection solution to
Stop data theft and targeted APT attacks**

ThreatSpect Bot Discovery Engine

1

Criminal's
Hideout



Detect Command
and Control
IP/URL/DNS

Over 250M
Addresses Analyzed
powered by ThreatCloud™

2

Criminal's
Communication



Detect Unique
Communication
Patterns

Over 2,000
Botnet Families!

3

Criminal's
Behavior

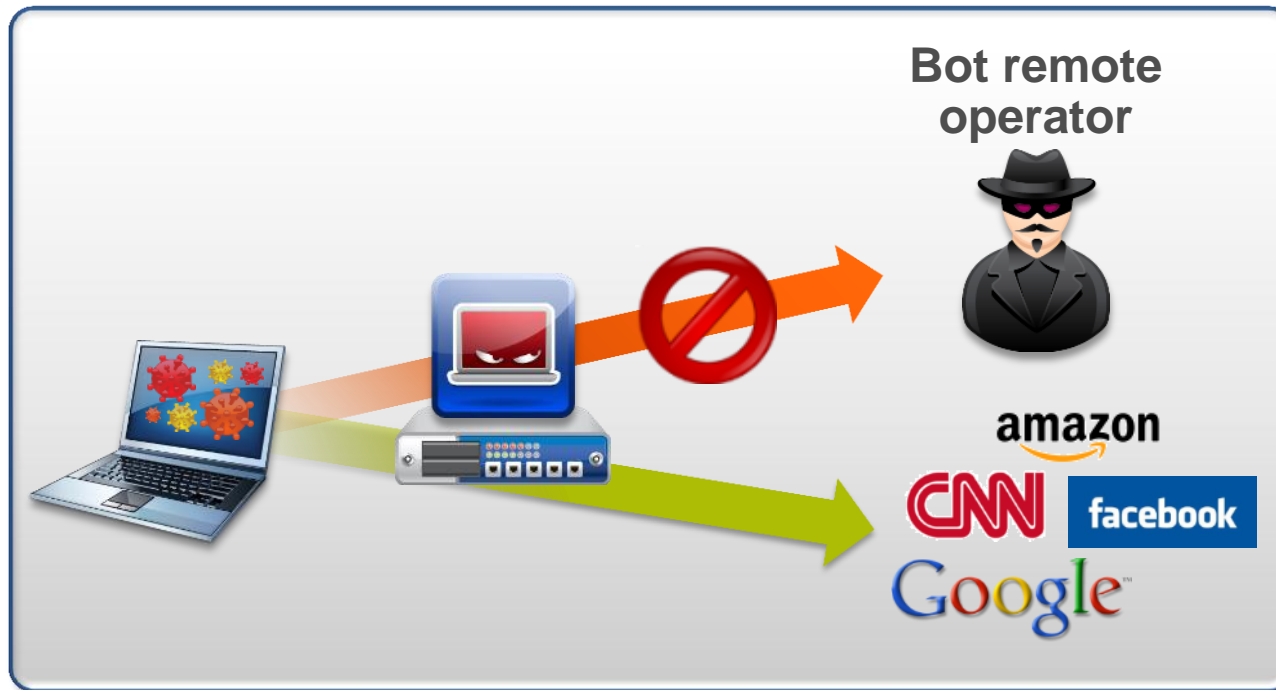


Detect Attack
Signs and Types
(spam, click fraud...)

Over 2 Million
Outbreaks
powered by ThreatCloud™



Stop Traffic between Infected Hosts and Remote Operator



**Stop
Data Theft**

**Enable User
Work Continuity**

**Performance
Over 40Gbps***

*40 Gbps on 61000 – Q3/12



Extensive Forensics Tools



**Infected Users
and Devices**



**Malware
Type**



**Malware
Actions**

 **Bot Incident:**  Prevent

 Copy Details  Actions  Anti-Bot Summary Details

 Frances Flash

 [Backdoor.WIN32.IRCBotg](#)
(Signature)

 Prevented

 Communication with C&C

 High Severity

 High Confidence

 Today at 12:09:43

- Event Description:**
Malware Backdoor.WIN32.IRCBotg on  125.0.0.68 tried to locate its Command and Control server on  203.0.0.210 at 12:09:43 19 Mar 2012.
- Additional Data:**
Destination: [203.0.0.210](#)
Sent Bytes: 38 Bytes
Received Bytes: 112 Bytes

Multi Layered Threat Prevention – ThreatCloud™



**Global collaboration
to fight new threats**

**Powering Threat Prevention Software Blades
with real-time security intelligence**

Global Collaboration to Fight New Threats



Real-time Security Intelligence
Gateways are constantly synced and protected

Threat Cloud™ is Growing



Over **250 million**
addresses analyzed
for bots discovery

Over **12 million**
malware signatures

Over **1 million**
malware-infested sites

1,000 URL updates per **day!**
50,000 signature updates per **day!**

Multi Layered Threat Prevention – DDoS Protector



**Block Denial of
Service Attacks
Within Seconds!**



Network and Application layer DDoS Protection

Multi-Layer Solution

IPS

Prevent exploit
of known vulnerabilities



Antivirus

Block download of
known malware



Anti-Bot

Block Bot
Communication



?

Unknown Threats



**85% of breaches took
weeks or more to discover**

Verizon 2012
Data Breach Investigations Report

Introducing Check Point Threat Emulation



ADDING THE MISSING PIECE...



Fight Against Unknown Threats !

Stop targeted Zero-day attacks

Threat Emulation – Step by Step

Download file
sent to Threat
Emulation

File Inspected
in virtual
sandbox

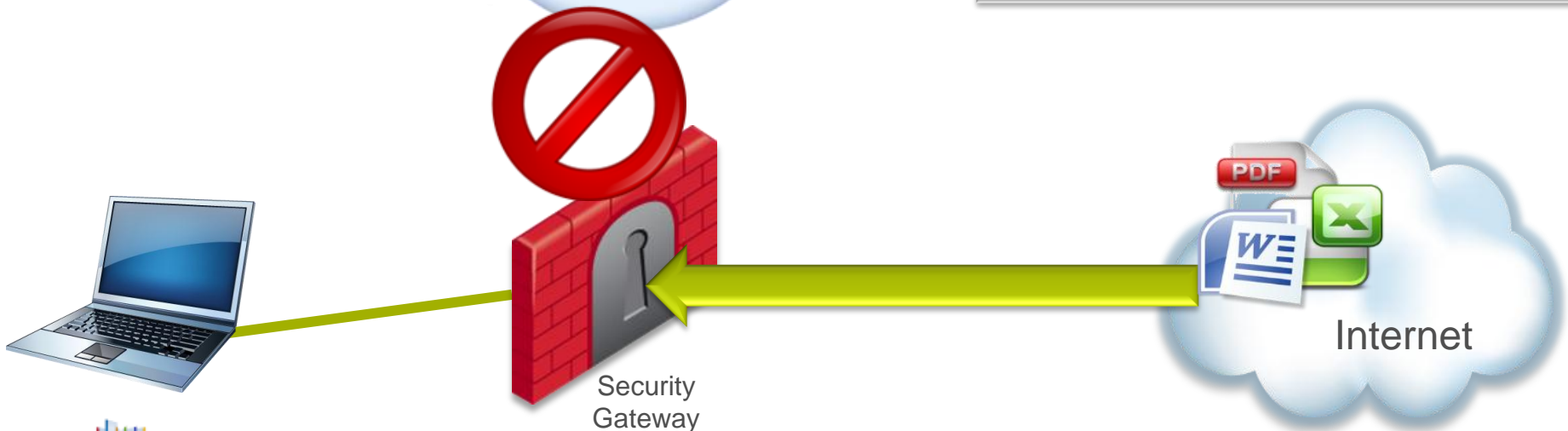
New attack
discovered

Malware is
blocked on
the gateway

New malware
signature sent
to ThreatCloud



- **Monitor unexpected behavior:**
 - **Network activity**
 - **File system & registry changes**
 - **Process activity**



Real Detection – Syrian Attack

MALWARE REPORT

Emulated on Windows XP 32bit SP1 Office 2003

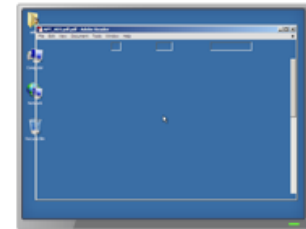
Generated by Threat Emulation®, on Wed Dec 26 14:16:48 2012

1

syrian.pdf Malicious Activity Detected

Type  PDF
Sender **eli@walla.co.il**
Recipient **moshe@walla.co.il**

Subject **Check this out**
MD5 **cb176a32de0738fea7073b 4d**
SHA1 **a7081468673e804fb88950**



**Detected by
Threat Emulation**

37 Affected Files 9 Files Created | 28 Files Modified | 1 Files Deleted

C:\\$ConvertToNonresident
C:\Documents and Settings\admin\Local Settings\Temp\1.dat
C:\Documents and Settings\admin\Local Settings\Temp\964.PDF
C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe
[33 More](#)

3 Affected Registry Keys 1 Set Entries | 2 Deleted Entries

**Drops malware
(Temp directory)**

Executes the malware

1 Affected Processes 1 Processes Created | 0 Processes Terminated | 0 Processes Crashed

C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe

1 Attempted Network Connections

sureshreddy1.dns05.com

Contact CnC

Summary – Check Point Multi Layered Threat Prevention





**Unmatched multi-layered security
against known and unknown threats**

**Multiple bot and malware detection
engines leading to superior protection**

**Real-time security intelligence ensuring
your gateway constantly protected**

**Stopping unknown 0-day attacks without
sending sensitive data to the cloud**

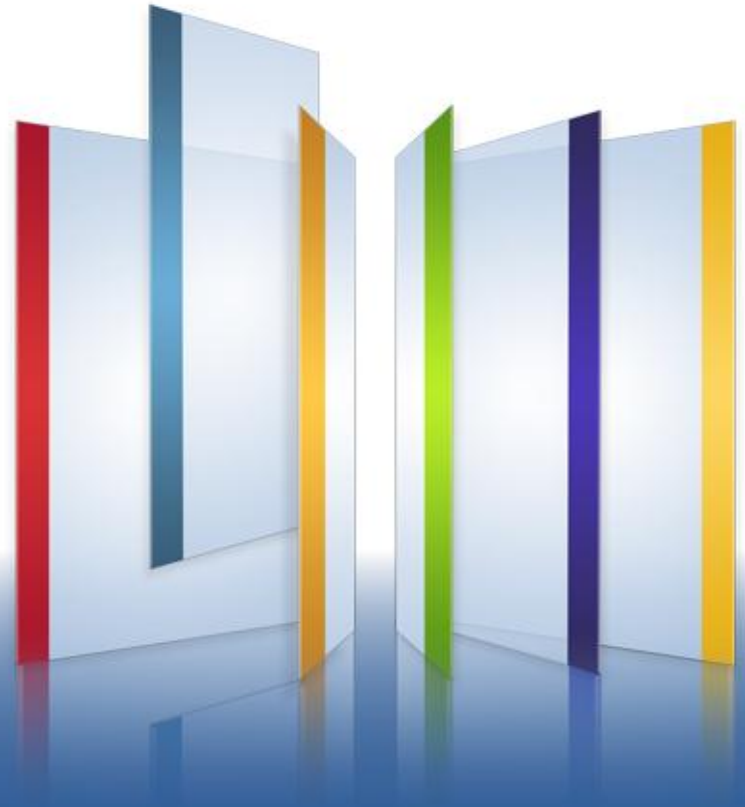
**Block DDoS attacks within seconds with
network and application layer security**



Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

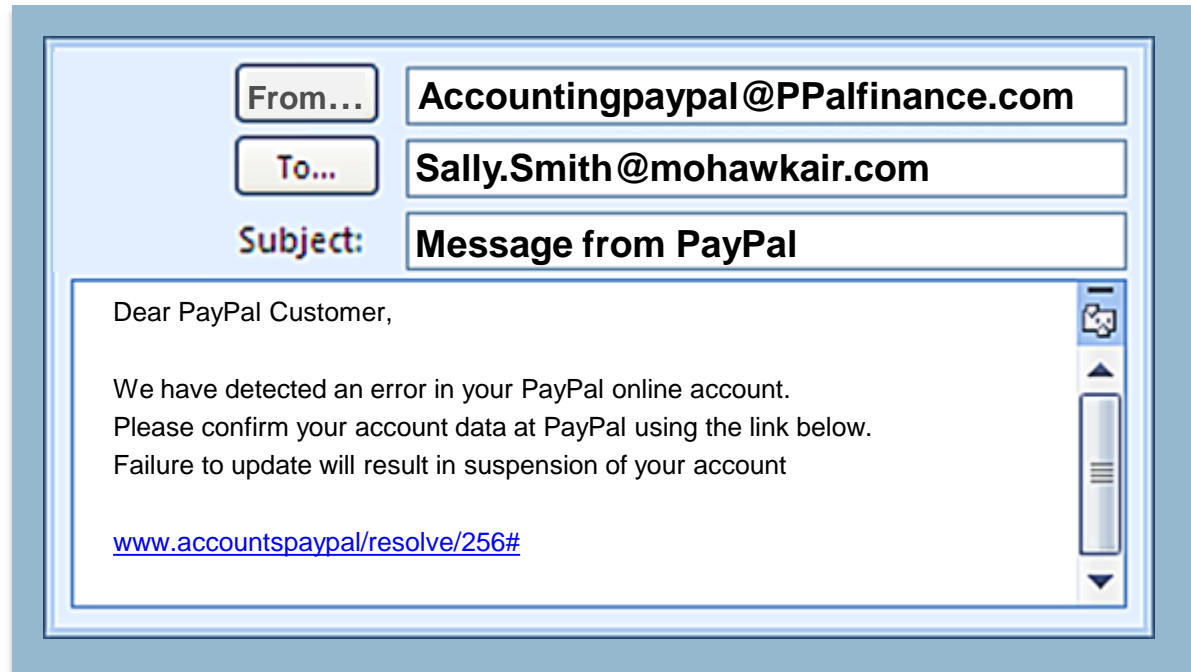
Thank You



Malware Prevention Scenario



While reading email, Sally clicks on link





Zbot attempts to infect Sally's computer


Antivirus Software Blade blocks attack





Virus Incident: Prevent Copy Details Actions Anti-Virus Summary


 Sally Smith


 Trojan-Spy.MSIL.ZBOT.agi (Signature)

 Prevented



 Malicious file/exploit download

 Critical Severity

 High Confidence

 24 Mar 2012 at 13:54:02

Event Description:

A Malware on machine  75.0.0.253 attempted to locate and download a malicious file from  80.0.0.68 at 13:54:02 24 Mar 2012.

Additional Data:

Destination: [80.0.0.68](#)

Sent Bytes: 23 KB

Received Bytes: 193 KB

Zbot Trojan is loaded onto a USB stick




Bob plugs the USB stick into his computer and the trojan is installed

**Zbot turns
Bob's computer into a bot**

Anti-Bot Software Blade detected and blocked Zbot trying to communicate with a C&C server




Bot Incident: Prevent Copy Details Actions Anti-Bot Summary De


 Bob Jager


 Trojan-Spy.MSIL.ZBOT.agi (Signature)

 Prevented



 Communication with C&C

 High Severity

 High Confidence

 Today at 12:09:43

Event Description:

Malware Backdoor.WIN32.IRCBotg on  125.0.0.68 tried to locate its Command and Control server on  203.0.0.210 at 12:09:43 19 Mar 2012.

Additional Data:

Destination: [203.0.0.210](#)

Sent Bytes: 38 Bytes

Received Bytes: 112 Bytes

Bot Command & Control

Bot Name

Actions

Severity

Unified Anti-Malware defense

Policy

Add Rule ▾ Add Exception ▾ Delete ✕ Actions ▾ | Install Policy

No	Name	Protected Scope	Action	Track
1	Internal Net	+ internal_network	Recommended_Profile	Log
2	WiFi Net	+ WiFi_Net		Log
3	Finance Net	Finance_Server Finance_Users_Role Corporate-finance-ne		Capture

Name: Recommended_Profile

Comment: Anti-Bot and Antivirus

Protection Activation Policy

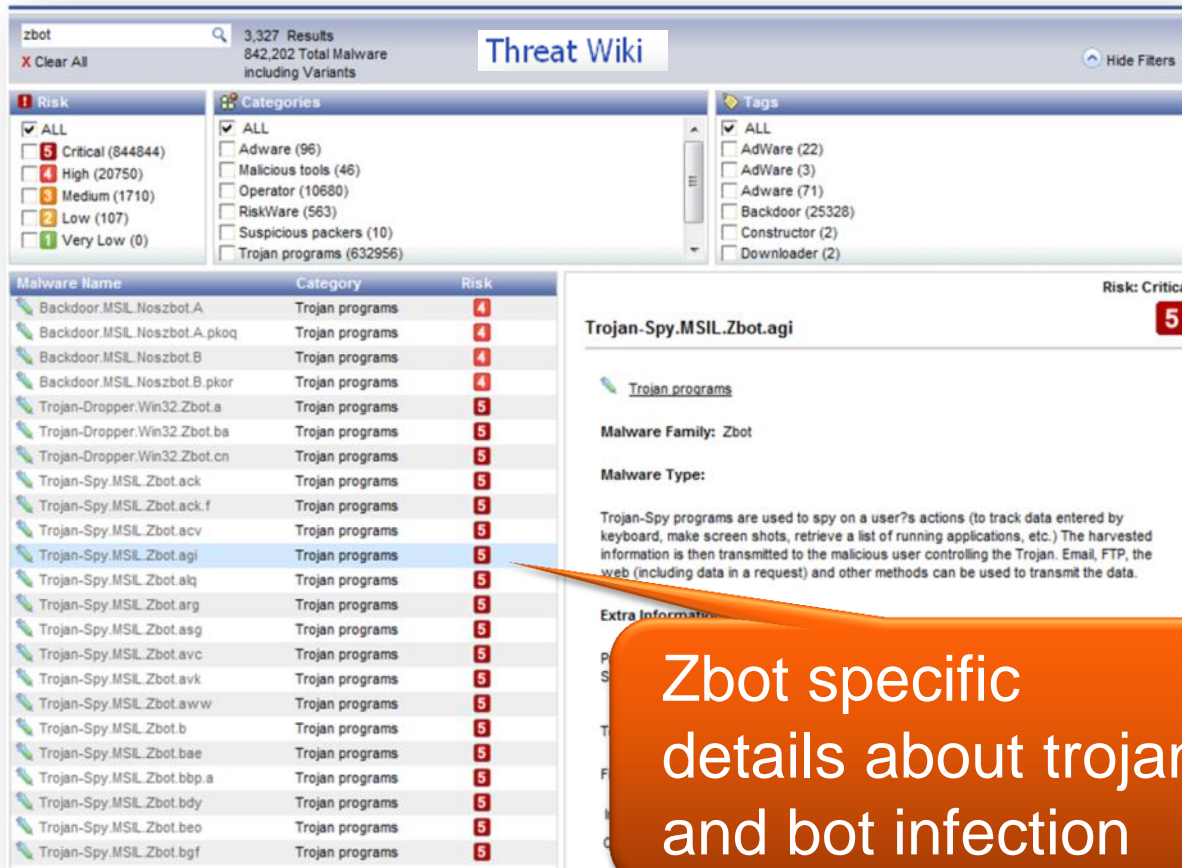
High Confidence: Prevent

Medium Confidence: Prevent

Low Confidence: Detect

Performance Impact: Medium or lower

Detailed reference for understanding attack severity, possible damage and removal procedures



zbot 3,327 Results
842,202 Total Malware including Variants

Threat Wiki

Hide Filters

Risk

- ☒ ALL
- ☐ Critical (844844)
- ☐ High (20750)
- ☐ Medium (1710)
- ☐ Low (107)
- ☐ Very Low (0)

Categories

- ☒ ALL
- ☐ Adware (96)
- ☐ Malicious tools (46)
- ☐ Operator (10680)
- ☐ RiskWare (563)
- ☐ Suspicious packers (10)
- ☐ Trojan programs (632956)

Tags

- ☒ ALL
- ☐ AdWare (22)
- ☐ AdWare (3)
- ☐ Adware (71)
- ☐ Backdoor (25328)
- ☐ Constructor (2)
- ☐ Downloader (2)

Malware Name	Category	Risk
Backdoor.MSIL.Noszbot.A	Trojan programs	4
Backdoor.MSIL.Noszbot.A.pkoq	Trojan programs	4
Backdoor.MSIL.Noszbot.B	Trojan programs	4
Backdoor.MSIL.Noszbot.B.pkor	Trojan programs	4
Trojan-Dropper.Win32.Zbot.a	Trojan programs	5
Trojan-Dropper.Win32.Zbot.ba	Trojan programs	5
Trojan-Dropper.Win32.Zbot.cn	Trojan programs	5
Trojan-Dropper.Win32.Zbot.ct	Trojan programs	5
Trojan-Spy.MSIL.Zbot.ack	Trojan programs	5
Trojan-Spy.MSIL.Zbot.ack.f	Trojan programs	5
Trojan-Spy.MSIL.Zbot.acv	Trojan programs	5
Trojan-Spy.MSIL.Zbot.agi	Trojan programs	5
Trojan-Spy.MSIL.Zbot.alq	Trojan programs	5
Trojan-Spy.MSIL.Zbot.arg	Trojan programs	5
Trojan-Spy.MSIL.Zbot.asg	Trojan programs	5
Trojan-Spy.MSIL.Zbot.avc	Trojan programs	5
Trojan-Spy.MSIL.Zbot.avk	Trojan programs	5
Trojan-Spy.MSIL.Zbot.aww	Trojan programs	5
Trojan-Spy.MSIL.Zbot.b	Trojan programs	5
Trojan-Spy.MSIL.Zbot.bae	Trojan programs	5
Trojan-Spy.MSIL.Zbot.bbp.a	Trojan programs	5
Trojan-Spy.MSIL.Zbot.bdy	Trojan programs	5
Trojan-Spy.MSIL.Zbot.beo	Trojan programs	5
Trojan-Spy.MSIL.Zbot.bgf	Trojan programs	5

Trojan-Spy.MSIL.Zbot.agi Risk: Critical 5

Trojan programs

Malware Family: Zbot

Malware Type:

Trojan-Spy programs are used to spy on a user's actions (to track data entered by keyboard, make screen shots, retrieve a list of running applications, etc.) The harvested information is then transmitted to the malicious user controlling the Trojan. Email, FTP, the web (including data in a request) and other methods can be used to transmit the data.

Extra Information

Zbot specific details about trojan and bot infection