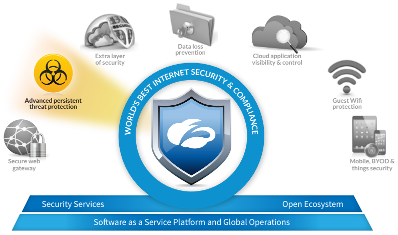
zscaler®

DATASHEET

Zscaler® Advanced Persistent Threat Protection™


Extra layer of security
Data loss prevention
Cloud application visibility & control
Advanced persistent threat protection
Guest Wifi protection
Secure web gateway
Mobile, BYOD & things security
WORLD'S BEST INTERNET SECURITY & COMPLIANCE
Security Services
Open Ecosystem
Software as a Service Platform and Global Operations

THE ZSCALER PLATFORM

Zscaler's award-winning Security as a Service platform delivers a safe and productive Internet experience for every user, from any device and from any location. Zscaler effectively moves security into the Internet backbone, operating in more than 100 data centers around the world and enabling organizations to fully leverage the promise of cloud and mobile computing with unparalleled and uncompromising protection and performance. Zscaler delivers unified, carrier-grade Internet security, advanced persistent threat (APT) protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence–all without the need for on-premise hardware, appliances or software.

WHAT DO OUR CUSTOMERS THINK?

MAN Diesel & Turbo

"It seems a single day doesn't pass without some interesting new botnet emerging in the news...it's reassuring to know that Zscaler for APTs leverages the depth of its behavioral analysis with the breadth of its Security as a Service platform to deliver a uniquely comprehensive solution."

- **Tony Ferguson**, IT Architect

Zscaler Advanced Persistent Threat Protection delivers defense-in-depth against APTs.

Zscaler APT Protection provides full lifecycle protection against Advanced Persistent Threats (APTs) that goes far beyond just "signatureless" detection, with a comprehensive defense-in-depth approach. And because it's delivered on top of the Zscaler Security as a Service platform, enterprises can now truly protect against APTs at all locations and for all users and devices, with an easy and cost effective solution.

Defense-in-depth, in-line and automated

Hackers are coming after your people, systems, and data with custom-tailored APT attacks designed to exploit your vulnerabilities and bypass your existing security. With Zscaler APT Protection, you can now protect your users from these sophisticated threats with a multi-layered **"protect-detect-remediate"** defense framework, including advanced "signatureless" behavioral analysis, sandboxing and forensics capabilities. And unlike most security appliances, Zscaler sits in-line with your Internet traffic, bi-directionally inspecting every byte including SSL and automatically blocking malware, infected devices, and data exfiltration.

Protect headquarters, branches and road warriors, all from the cloud

APT attackers research and target the most vulnerable parts of your infrastructure and many organizations have critical gaps in protecting remote offices, road warriors, mobile devices and Internet-connected things. Zscaler APT Protection is designed to protect all of your users and all of your systems, wherever on the planet they happen to be located–from the cloud. Our massive cloud-based security platform has 12 million users and sees 12 billion transactions a day, so we can deliver the fastest threat analysis, the highest catch rates coupled with the lowest false positives and the fastest time to block threats across our user network.

Improve your security posture, while lowering costs

The traditional way to address enterprise security has been to stack security appliances at each of your Internet gateways–an approach that has proven to be complex, expensive, and prone to security gaps. Zscaler delivers multi-layered security from the cloud, consolidating a broad set of security appliances into a single integrated Security as a Service platform. As a result, Zscaler customers see improved administrator productivity, reduced capex and opex, reduced bandwidth costs, improved network performance, and reduced security event expenditures. The bottom line–Zscaler costs just pennies per employee per day—four times less than purchasing and running your own security appliances.

PROTECT

Stop infections from happening by identifying and blocking zero day malware, worms, viruses, trojans, malicious IPs and URLs...

PROTECT
DETECT
REMEDIATE

DETECT

Identify compromised devices sending command & control communications, botnet traffic, and trying to exfiltrate data.

REMEDIATE

Minimize and heal the impact of APT attacks by locating, blocking, and fixing compromised devices.

Zscaler defense-in-depth framework

PROTECT:

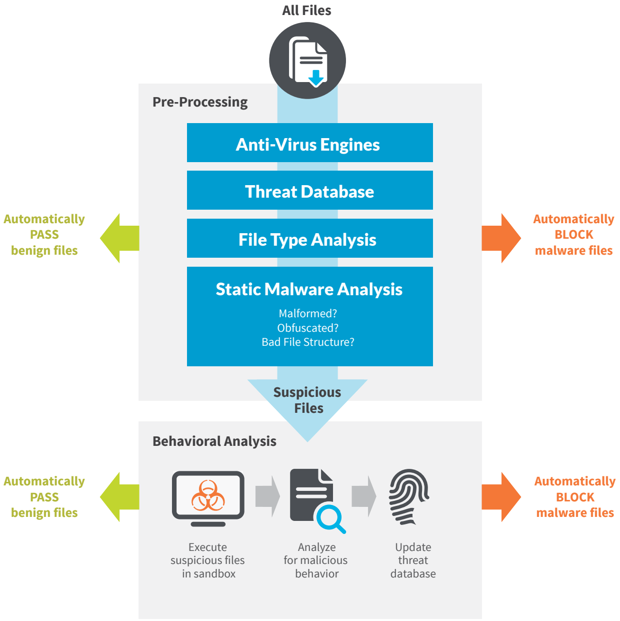
Stop infections from happening

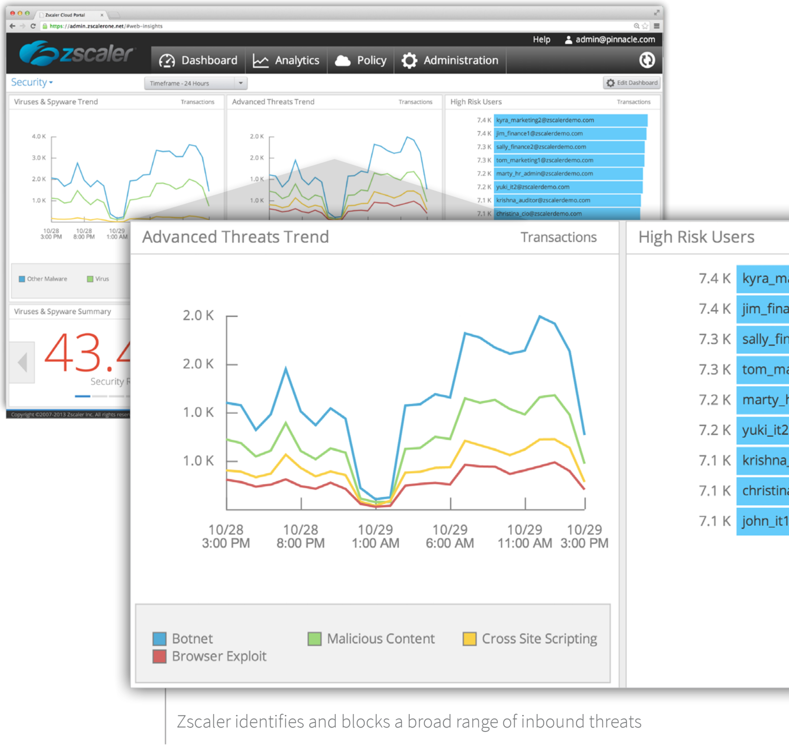
Inspect and block threats with inline scanning

Leveraging a purpose-built architecture capable of high-speed bi-directional content inspection, Zscaler scans all Internet traffic in real time, automatically blocking threats when they are identified.

Inspect ALL Internet traffic, including SSL

Zscaler, as a 100% cloud service, seamlessly integrates SSL traffic inspection into our bi-directional inline scanning without any deterioration in performance or requiring any additional hardware or software. Since Zscaler is always deployed in-line, we can always take action on SSL encrypted content.





7.4 K	kyra_marketing2@zscalerdemo.com
7.4 K	jim_finance1@zscalerdemo.com
7.3 K	sally_finance2@zscalerdemo.com
7.3 K	tom_marketing1@zscalerdemo.com
7.2 K	marty_hr_admin@zscalerdemo.com
7.2 K	yuki_it2@zscalerdemo.com
7.1 K	krishna_auditor@zscalerdemo.com
7.1 K	christina_cio@zscalerdemo.com
7.1 K	john_it1

Zscaler identifies and blocks a broad range of inbound threats

Stop zero-day attacks with behavioral analysis

Suspicious objects are automatically executed and monitored in a controlled sandbox and any malicious behaviors are recorded and analyzed. Malicious objects are automatically blocked across all 12 million of our customers and all of this happens in near real time. Suspicious content can be quarantined until analyzed, so even the first person who attempts to download a malicious object will be protected.

Stop known malware threats

Zscaler inspects and protects against known viruses and worms using multiple signature and heuristic technologies. Our cloud architecture provides inspection at many times the speed of on premise products, ensuring full protection without introducing material latency.

Shut down browser vulnerabilities

To avoid exposing known vulnerabilities to potential attackers, Zscaler browser control enforces policies that limit Internet access to specific browser versions, patch levels, allowed plug-ins and applications.

Stop known malicious URL threats

Zscaler blocks user access to malicious web sites by identifying requests to known malicious URLs. Because Zscaler sees more than 12 billion web requests each and every day, we can identify a threat targeting one of our customers and instantaneously leverage that knowledge to protect our entire network.

DETECT:

Identify compromised devices

Identify communications by compromised devices

Leveraging our bi-directional deep inspection capabilities, Zscaler monitors outbound traffic (including SSL) to identify communications by infected machines. This includes interactions with known botnet command and control ("C&C") servers, communications by infected machines using P2P applications to avoid detection, and traffic to suspicious destinations or countries.

Identify data exfiltration attempts

To help detect data exfiltration, Zscaler scans all Internet-bound traffic (including content encrypted over SSL) to identify sensitive or unauthorized data, including credit cards, SSNs, financial statements, customer information, medical documents, source code, and other intellectual property.

Identify botnet and stealth behavior

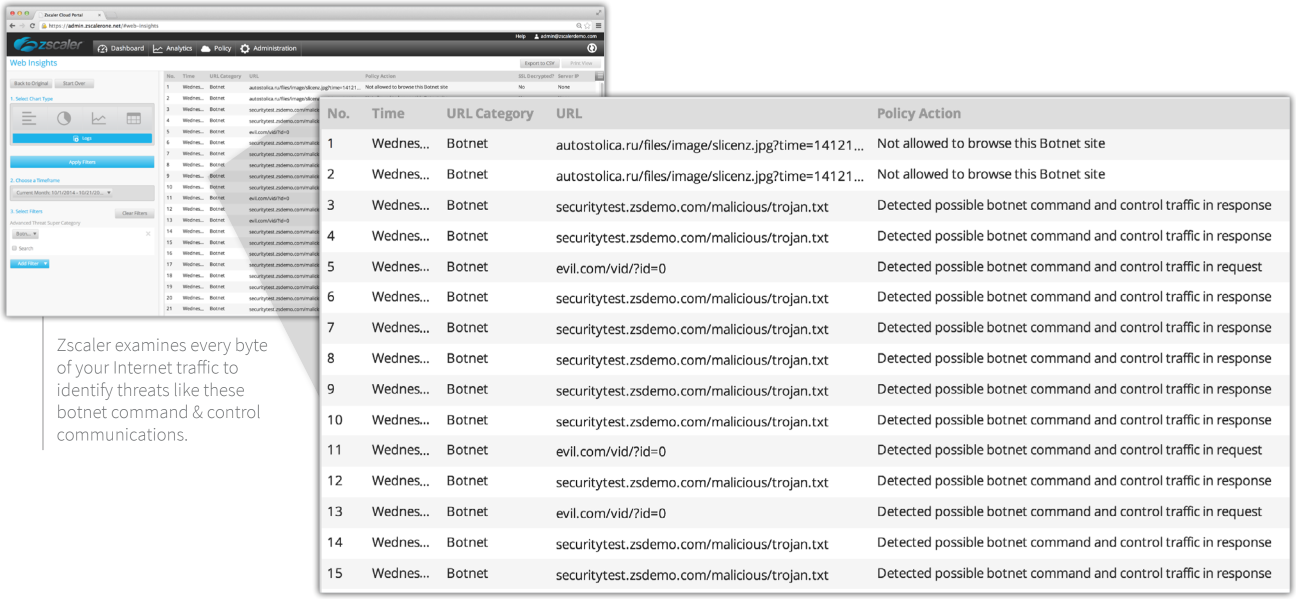
Attackers use a variety of techniques (e.g., Fast Flux) to set up their command-and-control servers and keep them under the radar. Zscaler analyzes Internet traffic to identify suspicious domains such as very young domains (e.g. less than 24 hours old), odd domains that only a few IP addresses are querying, and patterns of failed domain lookups.

Leverage cloud data to identify C&C servers

Zscaler Labs conducts ongoing analysis and data mining of traffic patterns for malware found in the wild across our 12+ million customers and 12+ billion daily transactions, to uncover and block command and control servers associated with these attacks.

Alert on suspicious port/protocol usage

Zscaler can identify and send out alerts based on unusual port or protocol usage patterns that indicate an infection or compromise.



No.	Time	URL Category	URL	Policy Action
1	Wednes...	Botnet	autostolica.ru/files/image/slicenz.jpg?time=14121...	Not allowed to browse this Botnet site
2	Wednes...	Botnet	autostolica.ru/files/image/slicenz.jpg?time=14121...	Not allowed to browse this Botnet site
3	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
4	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
5	Wednes...	Botnet	evil.com/vid/?id=0	Detected possible botnet command and control traffic in request
6	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
7	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
8	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
9	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
10	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
11	Wednes...	Botnet	evil.com/vid/?id=0	Detected possible botnet command and control traffic in request
12	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
13	Wednes...	Botnet	evil.com/vid/?id=0	Detected possible botnet command and control traffic in request
14	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response
15	Wednes...	Botnet	securitytest.zsdemo.com/malicious/trojan.txt	Detected possible botnet command and control traffic in response

Zscaler examines every byte of your Internet traffic to identify threats like these botnet command & control communications.

REMEDIATE:

Minimize and heal the impact of APTs

Block data exfiltration

To stop data exfiltration, Zscaler automatically blocks all Internet-bound traffic (including SSL) containing unauthorized content.

Stop unauthorized communications

Zscaler also locks down unauthorized ports, protocols and cloud applications to make sure attackers can't use these channels for communications or data exfiltration.

Block communications by infected devices

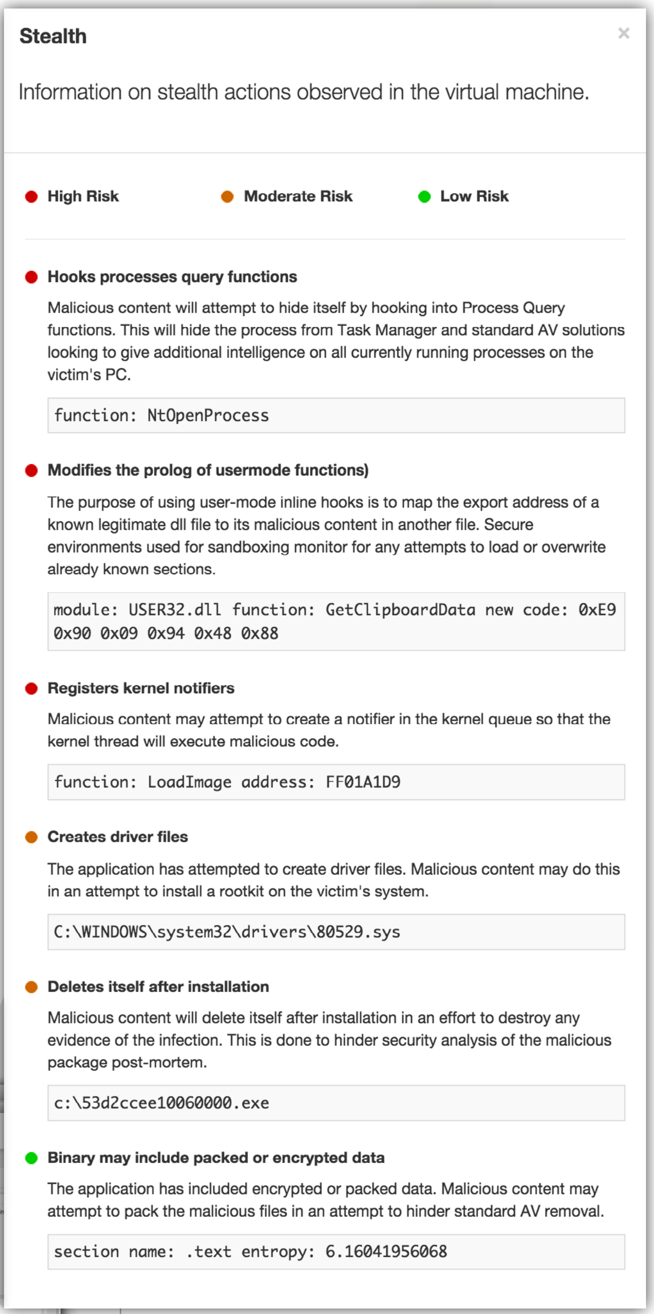
Zscaler's inline scanning identifies and automatically blocks communications by infected machines, including botnet command and control ("C&C") servers, communications by infected machines using P2P applications to avoid detection, and traffic to suspicious destinations or countries.

Understand malware behavior for remediation

In analyzing APT attack behavior, Zscaler provides easy-to-use detailed forensic information on zero-day malware, including security bypass techniques, network activity, persistence techniques (to evade destruction attempts), detection evading techniques, system and file configuration changes, memory and process analysis, packet captures for detailed analysis, and origin and destination analysis for suspect locations. Zscaler can record and replay the attack behavior it saw as malware was executing.

Locate infected devices and understand attack patterns

With Zscaler's Advanced Cloud Security Analytics, IT professionals can view log histories, and correlate data across users, devices, locations and applications. Every transaction from every user around the globe is available in seconds, not minutes or even days as is the case with batch reports. And Zscaler integrates with the industry's leading SIEM products to provide the insights needed for better attack correlation and vector analysis.



Stealth ×

Information on stealth actions observed in the virtual machine.

● High Risk ● Moderate Risk ● Low Risk

● **Hooks processes query functions**

Malicious content will attempt to hide itself by hooking into Process Query functions. This will hide the process from Task Manager and standard AV solutions looking to give additional intelligence on all currently running processes on the victim's PC.

```
function: NtOpenProcess
```

● **Modifies the prolog of usermode functions)**

The purpose of using user-mode inline hooks is to map the export address of a known legitimate dll file to its malicious content in another file. Secure environments used for sandboxing monitor for any attempts to load or overwrite already known sections.

```
module: USER32.dll function: GetClipboardData new code: 0xE9
0x90 0x09 0x94 0x48 0x88
```

● **Registers kernel notifiers**

Malicious content may attempt to create a notifier in the kernel queue so that the kernel thread will execute malicious code.

```
function: LoadImage address: FF01A1D9
```

● **Creates driver files**

The application has attempted to create driver files. Malicious content may do this in an attempt to install a rootkit on the victim's system.

```
C:\WINDOWS\system32\drivers\80529.sys
```

● **Deletes itself after installation**

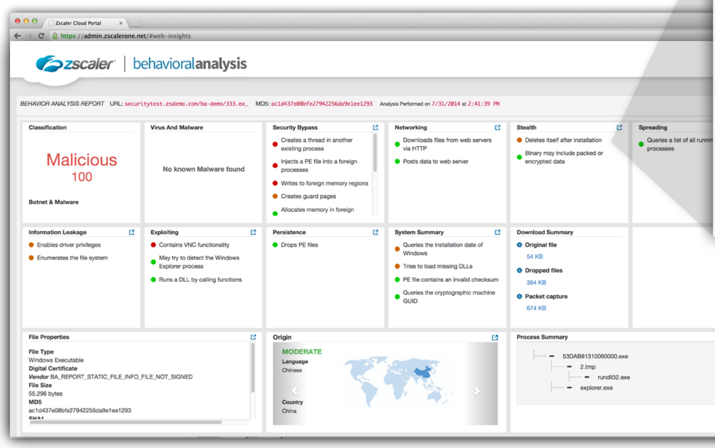
Malicious content will delete itself after installation in an effort to destroy any evidence of the infection. This is done to hinder security analysis of the malicious package post-mortem.

```
c:\53d2ccee10060000.exe
```

● **Binary may include packed or encrypted data**

The application has included encrypted or packed data. Malicious content may attempt to pack the malicious files in an attempt to hinder standard AV removal.

```
section name: .text entropy: 6.16041956068
```


Zscaler Cloud Portal
https://admin.zscalerone.net/#web-insights
zscaler | behavioralanalysis

BEHAVIOR ANALYSIS REPORT URL: securitytest.zsdemo.com/ba-demo/333.ex_ MD5: ac1d437e08bfe27942256da9e1ee1293 Analysis Performed on 7/31/2014 at 2:41:39 PM

Classification
Malicious
100
Botnet & Malware

Virus And Malware
No known Malware found

Security Bypass
- ● Creates a thread in another existing process
- ● Injects a PE file into a foreign processes
- ● Writes to foreign memory regions
- ● Creates guard pages
- ● Allocates memory in foreign

Networking
- ● Downloads files from web servers via HTTP
- ● Posts data to web server

Stealth
- ● Deletes itself after installation
- ● Binary may include packed or encrypted data

Spreading
- ● Queries a list of all runnin processes

Information Leakage
- ● Enables driver privileges
- ● Enumerates the file system

Exploiting
- ● Contains VNC functionality
- ● May try to detect the Windows Explorer process
- ● Runs a DLL by calling functions

Persistence
- ● Drops PE files

System Summary
- ● Queries the installation date of Windows
- ● Tries to load missing DLLs
- ● PE file contains an invalid checksum
- ● Queries the cryptographic machine GUID

Download Summary
- Original file 54 KB
- Dropped files 394 KB
- Packet capture 674 KB

File Properties
File Type
Windows Executable
Digital Certificate
Vendor BA_REPORT_STATIC_FILE_INFO_FILE_NOT_SIGNED
File Size
55,296 bytes
MD5
ac1d437e08bfe27942256da9e1ee1293
SHA1

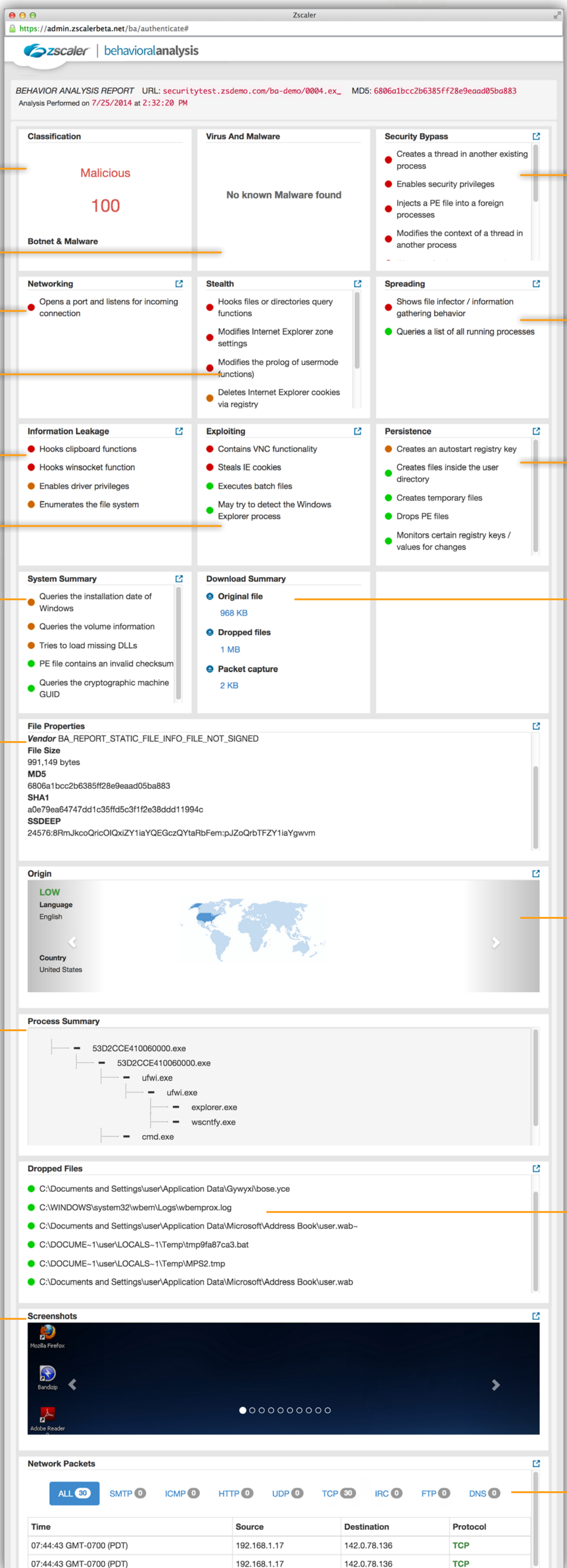
Origin
MODERATE
Language
Chinese
Country
China

Process Summary
```
├─ 53DAB81310060000.exe
   ├─ 2.tmp
   │  └─ rundll32.exe
   └─ explorer.exe
```

Zscaler behavioral analysis forensics provide the detailed malware insights necessary to identify and remediate compromised user devices.

Detailed Forensic Analysis of Zero-Day Malware

Zscaler Behavioral Analysis Reports provide a comprehensive analysis of the malicious behavior observed during execution of zero-day malware in our sandbox. Zscaler automatically blocks malware identified via Behavioral Analysis, maintaining a real time blacklist that prevents all users in our network from downloading malicious files.



Zscaler
https://admin.zscalerbeta.net/ba/authenticate#
zscaler | behavioralanalysis

BEHAVIOR ANALYSIS REPORT URL: securitytest.zsdemo.com/ba-demo/0004.ex_ MD5: 6806a1bcc2b6385ff28e9eaad05ba883
Analysis Performed on 7/25/2014 at 2:32:20 PM

Classification

Malicious

100

Botnet & Malware

Virus And Malware

No known Malware found

Security Bypass

- ● Creates a thread in another existing process
- ● Enables security privileges
- ● Injects a PE file into a foreign processes
- ● Modifies the context of a thread in another process

Networking

- ● Opens a port and listens for incoming connection

Stealth

- ● Hooks files or directories query functions
- ● Modifies Internet Explorer zone settings
- ● Modifies the prolog of usermode functions)
- ● Deletes Internet Explorer cookies via registry

Spreading

- ● Shows file infector / information gathering behavior
- ● Queries a list of all running processes

Information Leakage

- ● Hooks clipboard functions
- ● Hooks winsocket function
- ● Enables driver privileges
- ● Enumerates the file system

Exploiting

- ● Contains VNC functionality
- ● Steals IE cookies
- ● Executes batch files
- ● May try to detect the Windows Explorer process

Persistence

- ● Creates an autostart registry key
- ● Creates files inside the user directory
- ● Creates temporary files
- ● Drops PE files
- ● Monitors certain registry keys / values for changes

System Summary

- ● Queries the installation date of Windows
- ● Queries the volume information
- ● Tries to load missing DLLs
- ● PE file contains an invalid checksum
- ● Queries the cryptographic machine GUID

Download Summary

- **Original file**
  968 KB
- **Dropped files**
  1 MB
- **Packet capture**
  2 KB

File Properties

Vendor BA_REPORT_STATIC_FILE_INFO_FILE_NOT_SIGNED
File Size
991,149 bytes
MD5
6806a1bcc2b6385ff28e9eaad05ba883
SHA1
a0e79ea64747dd1c35ffd5c3f1f2e38ddd11994c
SSDEEP
24576:8RmJkcoQricOIQxiZY1iaYQEGczQYtaRbFem:pJZoQrbTFZY1iaYgwvm

Origin

LOW
Language
English
Country
United States

Process Summary

```
- 53D2CCE410060000.exe
    - 53D2CCE410060000.exe
        - ufwi.exe
            - ufwi.exe
                - explorer.exe
                - wscntfy.exe
        - cmd.exe
```

Dropped Files

- ● C:\Documents and Settings\user\Application Data\Gywyxi\bose.yce
- ● C:\WINDOWS\system32\wbem\Logs\wbemprox.log
- ● C:\Documents and Settings\user\Application Data\Microsoft\Address Book\user.wab~
- ● C:\DOCUME~1\user\LOCALS~1\Temp\tmp9fa87ca3.bat
- ● C:\DOCUME~1\user\LOCALS~1\Temp\MPS2.tmp
- ● C:\Documents and Settings\user\Application Data\Microsoft\Address Book\user.wab

Screenshots

Network Packets

Time	Source	Destination	Protocol
07:44:43 GMT-0700 (PDT)	192.168.1.17	142.0.78.136	TCP
07:44:43 GMT-0700 (PDT)	192.168.1.17	142.0.78.136	TCP

Overall classification of the file analyzed

Is the file a known piece of malware?

What kind of network traffic behavior does the file exhibit?

What kind of stealth or obfuscation behavior does the file exhibit?

Does the file leak or gather data during execution?

Does the file attempt to run exploits during execution?

Does the file gather system information during execution?

Detailed static information about the file

What are all the processes started by the file during execution?

Screenshot showing the computer user interface during file execution

Does the file try to bypass OS security?

Does the file try to gain wider access to the system or spread to other devices and computers?

What actions does the file take to create resistance to reboot and session lock?

What files are left behind after file execution?

Possible geographic origin of the file based on static analysis

List of the files created and left on the computer during file execution

Listing of all network traffic by protocol during file execution

Key Benefits

Protect against the full APT attack lifecycle with Zscaler's "protect-detect-remediate" defense-in-depth framework.

Protect

Identify and block zero-day and custom APT malware with "signatureless" behavior analysis.

Inspect ALL your Internet traffic with inline bi-directional scanning, including SSL.

Get instant protection once threats are detected, with inline scanning and automated blocking.

Protect users from risky or outdated software with browser vulnerability shielding.

Reduce alert fatigue with inline scanning and automated blocking.

Detect

Detect APT communications in your Internet traffic, including SSL encrypted streams.

Identify and immediately block command & control communications with APT attackers.

Identify and immediately block data exfiltration going out of your network.

Remediate

Quickly and easily find infections with correlated data across users, devices and locations.

Block command & control communications with APT attackers.

Block data exfiltration going out of your network.

Analyze and understand APT malware behavior with actionable and easy to use forensic data.

Zscaler Platform

- Get better security with lower TCO compared to appliance-centric approaches.
- Detect threats faster with lower false positives with cloud intelligence from 12+ million users and 12+ billion transactions per day.
- Deploy a proven security solution used by more than 5000 enterprise, government and military organizations, including General Electric, United Airlines, and Nestle.

About Zscaler

Zscaler ensures that more than 12 million employees at more than 5,000 enterprise and government organizations worldwide are protected against cyber attacks and data breaches while staying fully compliant with corporate and regulatory policies. Zscaler's award-winning Security as a Service platform delivers a safe and productive Internet experience for every user, from any device and from any location. Zscaler effectively moves security into the Internet backbone, operating in more than 100 data centers around the world and enabling organizations to fully leverage the promise of cloud and mobile computing with unparalleled and uncompromising protection and performance. Zscaler delivers unified, carrier-grade Internet security, advanced persistent threat (APT) protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence – all without the need for on-premise hardware, appliances or software. To learn more, visit us at **www.zscaler.com.**

CONTACT US

Zscaler, Inc.
110 Baytech Drive, Suite 100
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler-inc.
twitter.com/zscaler
youtube.com/zscalermarketing
zscaler.com/blogs.php