Check Point
SOFTWARE TECHNOLOGIES LTD

# CYBER SURVIVAL GUIDE

## Common Incident Response Cases

Gad Z. Naveh | Advanced Threat Prevention Evangelist

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

# Hacker’s GIT it

Check Point
SOFTWARE TECHNOLOGIES LTD

# We Don't

So you are moving to the cloud

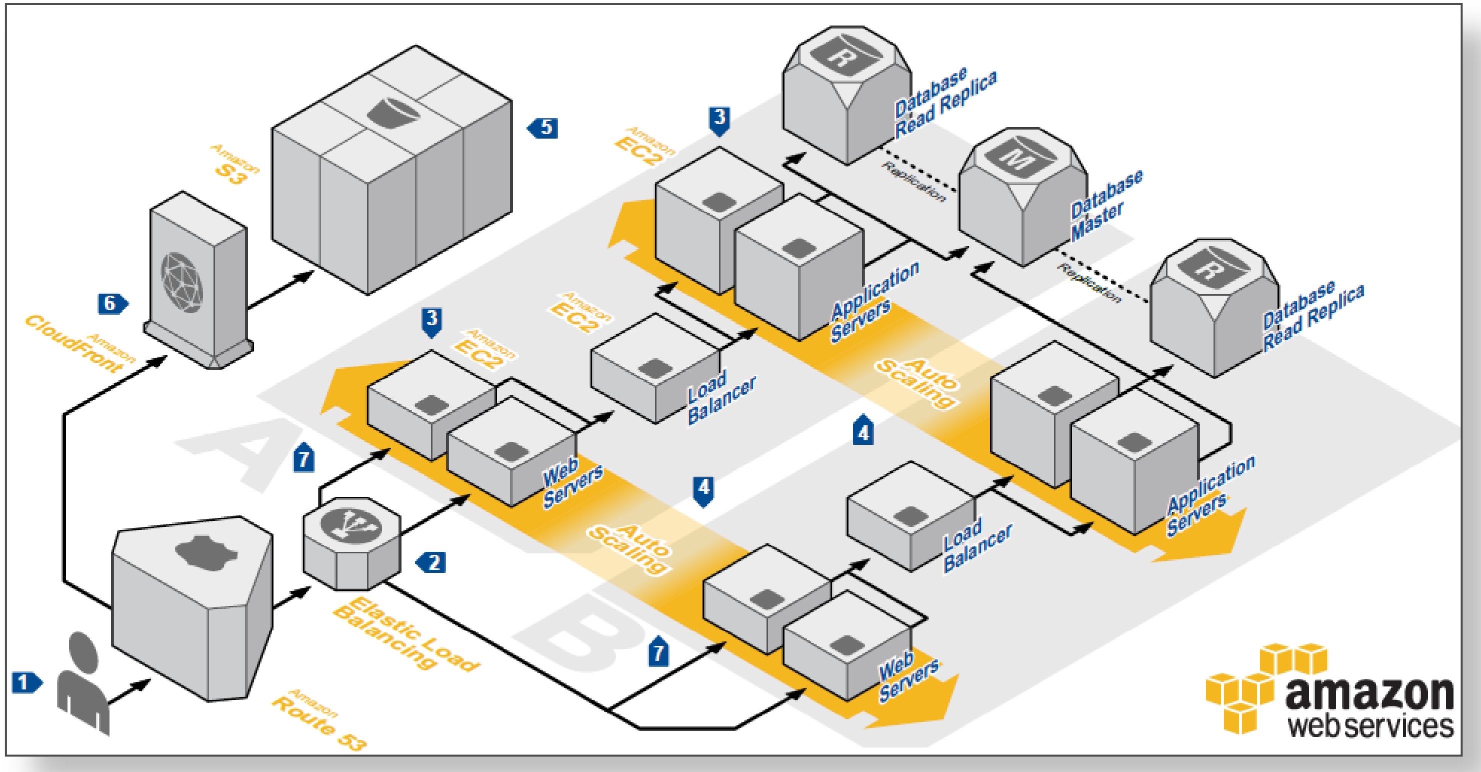
Let's start with the simple stuff

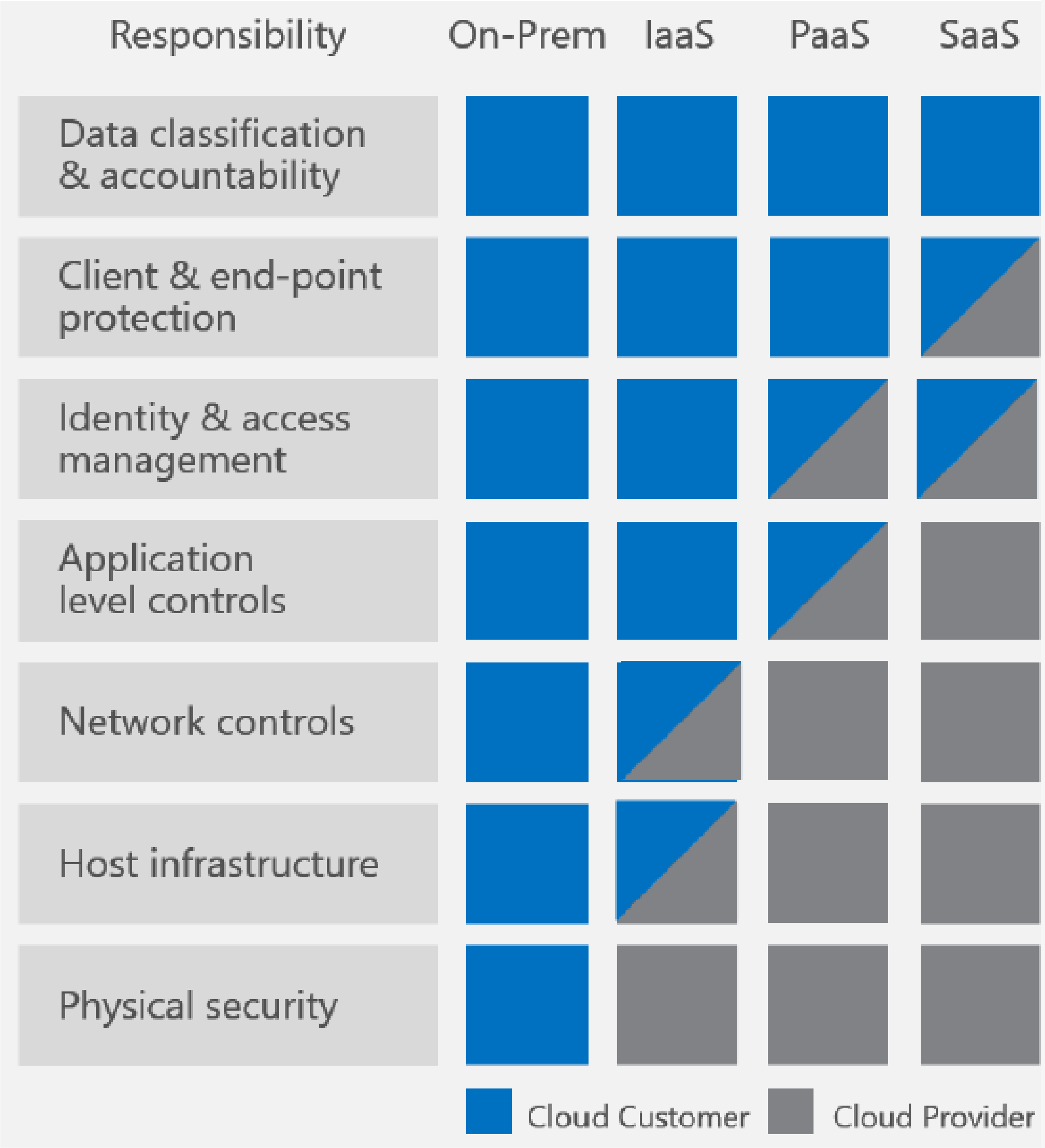
You start with a simple web infrastructure

Load Balancer with access control lists

Web Servers

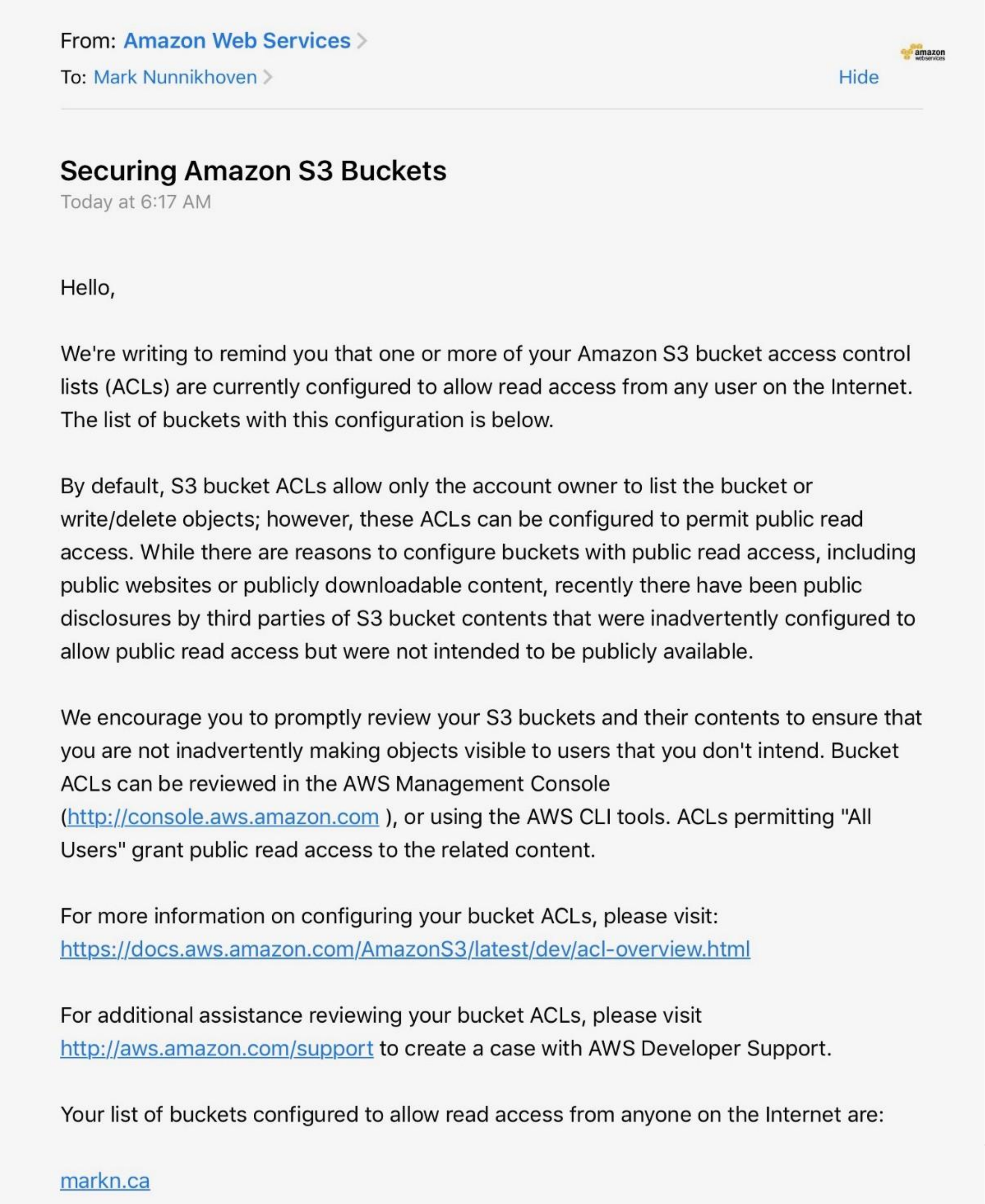
S3 Bucket for storage





| Responsibility | On-Prem | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Data classification & accountability | 🟦 | 🟦 | 🟦 | 🟦 |
| Client & end-point protection | 🟦 | 🟦 | 🟦 | ◩ |
| Identity & access management | 🟦 | 🟦 | ◩ | ◩ |
| Application level controls | 🟦 | 🟦 | ◩ | ⬛ |
| Network controls | 🟦 | ◩ | ⬛ | ⬛ |
| Host infrastructure | 🟦 | ◩ | ⬛ | ⬛ |
| Physical security | 🟦 | ⬛ | ⬛ | ⬛ |

🟦 Cloud Customer ⬛ Cloud Provider



From: Amazon Web Services

To: Mark Nunnikhoven

**Securing Amazon S3 Buckets**

Today at 6:17 AM

Hello,

We're writing to remind you that one or more of your Amazon S3 bucket access control lists (ACLs) are currently configured to allow read access from any user on the Internet. The list of buckets with this configuration is below.

By default, S3 bucket ACLs allow only the account owner to list the bucket or write/delete objects; however, these ACLs can be configured to permit public read access. While there are reasons to configure buckets with public read access, including public websites or publicly downloadable content, recently there have been public disclosures by third parties of S3 bucket contents that were inadvertently configured to allow public read access but were not intended to be publicly available.

We encourage you to promptly review your S3 buckets and their contents to ensure that you are not inadvertently making objects visible to users that you don't intend. Bucket ACLs can be reviewed in the AWS Management Console (http://console.aws.amazon.com ), or using the AWS CLI tools. ACLs permitting "All Users" grant public read access to the related content.

For more information on configuring your bucket ACLs, please visit: https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html

For additional assistance reviewing your bucket ACLs, please visit http://aws.amazon.com/support to create a case with AWS Developer Support.

Your list of buckets configured to allow read access from anyone on the Internet are:

markn.ca

Success, the environment Auto Scale's

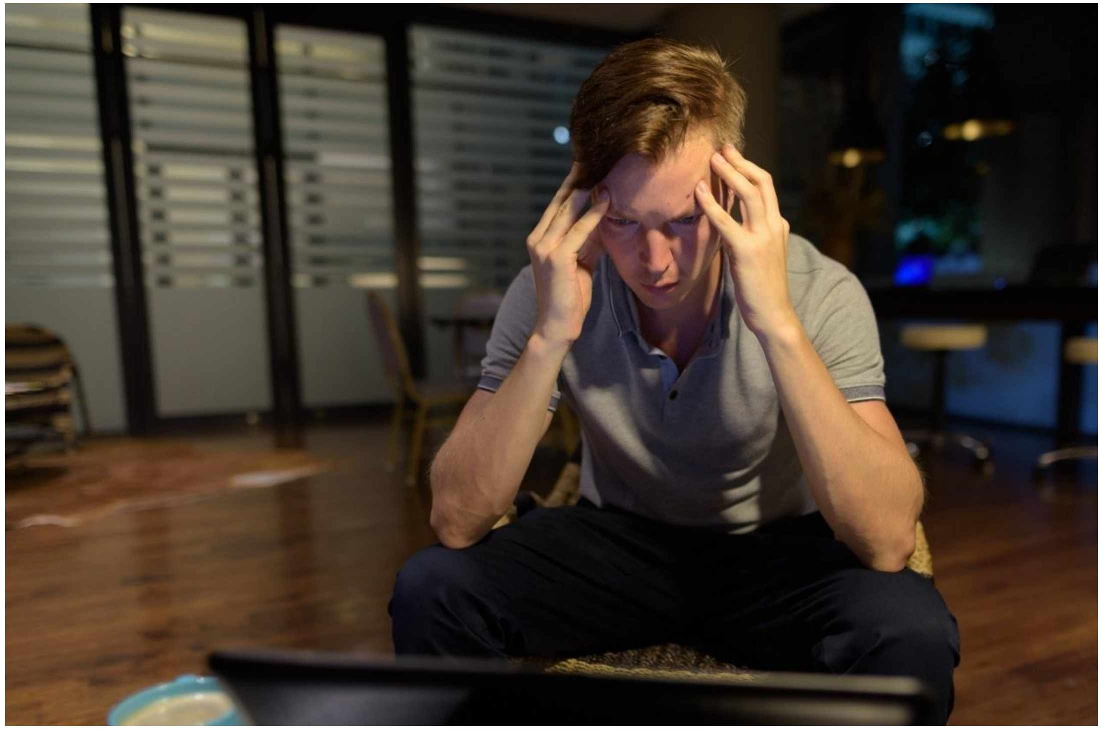
It gets bigger and bigger…

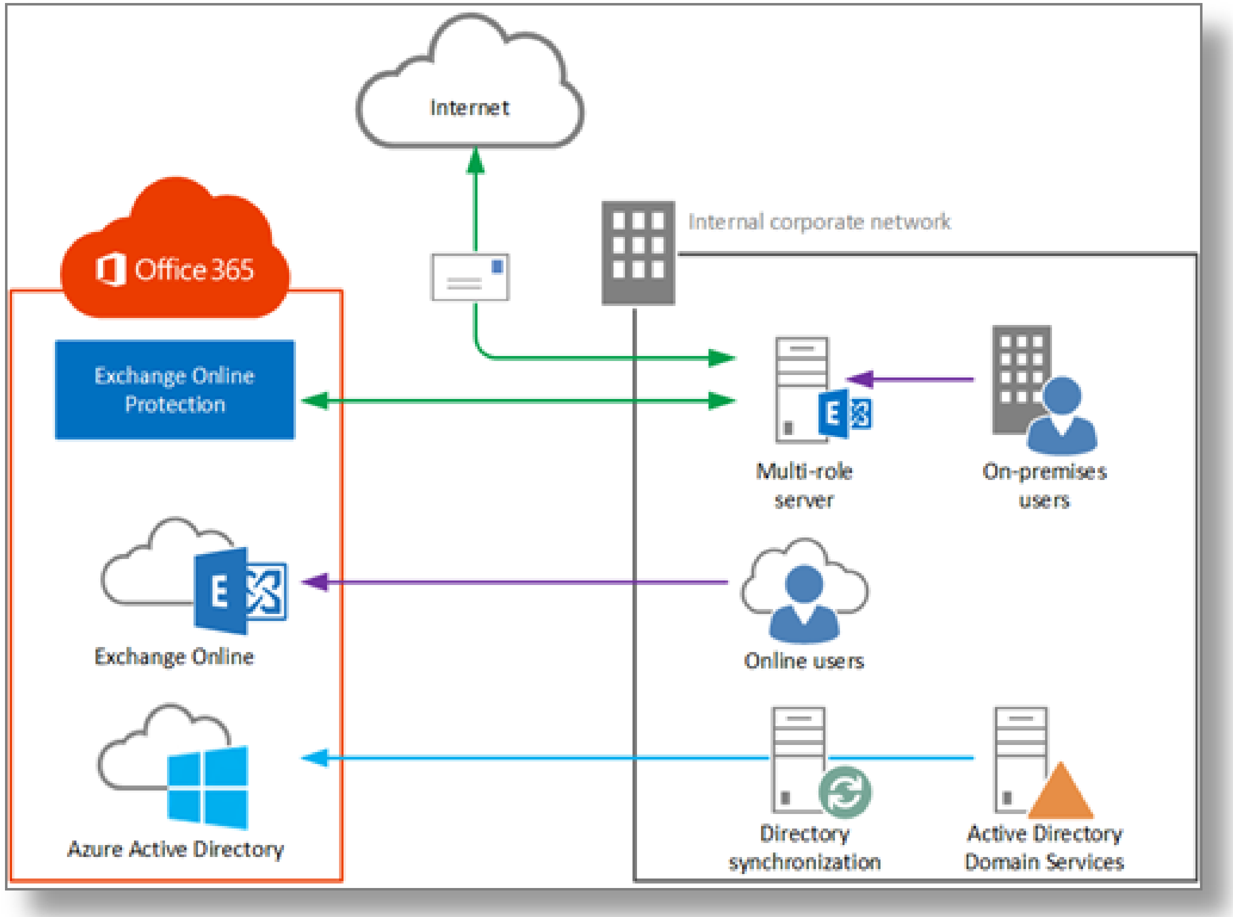
Costing more money

# JBoss management console exposed

Auto-Scaling Resource Consumption

# Let’s move more to the cloud!




Internet
Office 365
Exchange Online Protection
Internal corporate network
Multi-role server
On-premises users
Exchange Online
Online users
Azure Active Directory
Directory synchronization
Active Directory Domain Services

# Until one day you get a call…….

From: Accounts Payable

To: CFO

Subject: Urgent Payment

Hi Steve,

Please note that due invoice payment would be received to our subsidiary account as we have just been notified by our bank that our corporate account is audited and cannot accept any payments for now. Please use the following details for outstanding and future payments.

Acct Name: Send me money

BSB: 999999

Acct No: 1234567890

Kindly acknowledge receipt and understanding of message

## Let’s make some money from Email

Outbound SPAM

Data Theft

Whaling

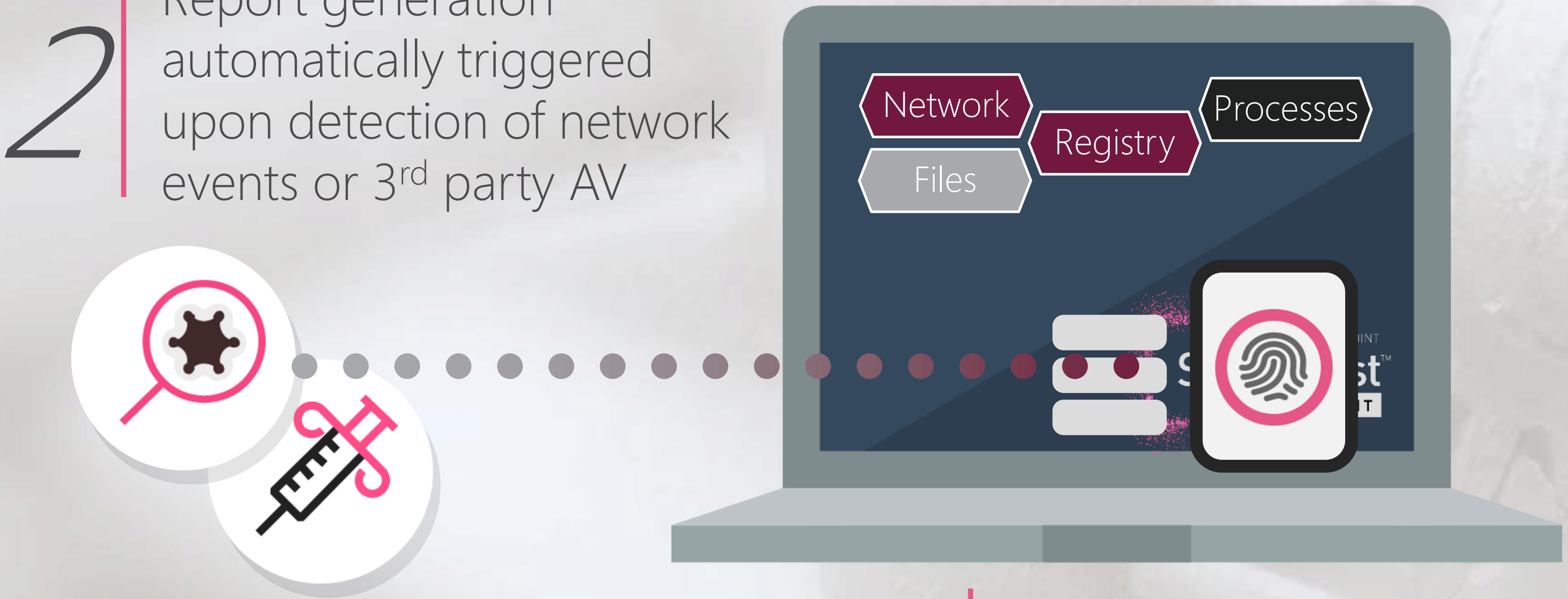
# Lateral Movement

# How Forensics Works

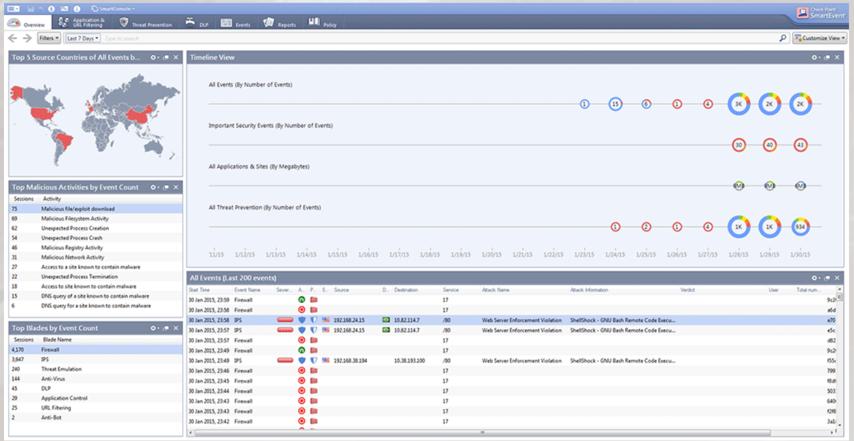
Check Point
SOFTWARE TECHNOLOGIES LTD

1 FORENSICS data continuously collected from various OS sensors

2 Report generation automatically triggered upon detection of network events or 3rd party AV



4 Digested incident report sent to SmartEvent



Top 5 Source Countries of All Events b...

Top Malicious Activities by Event Count

| Sessions | Activity |
|---|---|
| 75 | Malicious file/exploit download |
| 69 | Malicious Filesystem Activity |
| 62 | Unexpected Process Creation |
| 54 | Unexpected Process Crash |
| 46 | Malicious Registry Activity |
| 31 | Malicious Network Activity |
| 27 | Access to a site known to contain malware |
| 22 | Unexpected Process Termination |
| 18 | Access to site known to contain malware |
| 15 | DNS query of a site known to contain malware |
| 6 | DNS query for a site known to contain malware |

Top Blades by Event Count

| Sessions | Blade Name |
|---|---|
| 4,170 | Firewall |
| 3,647 | IPS |
| 240 | Threat Emulation |
| 144 | Anti-Virus |
| 45 | DLP |
| 29 | Application Control |
| 25 | URL Filtering |
| 2 | Anti-Bot |

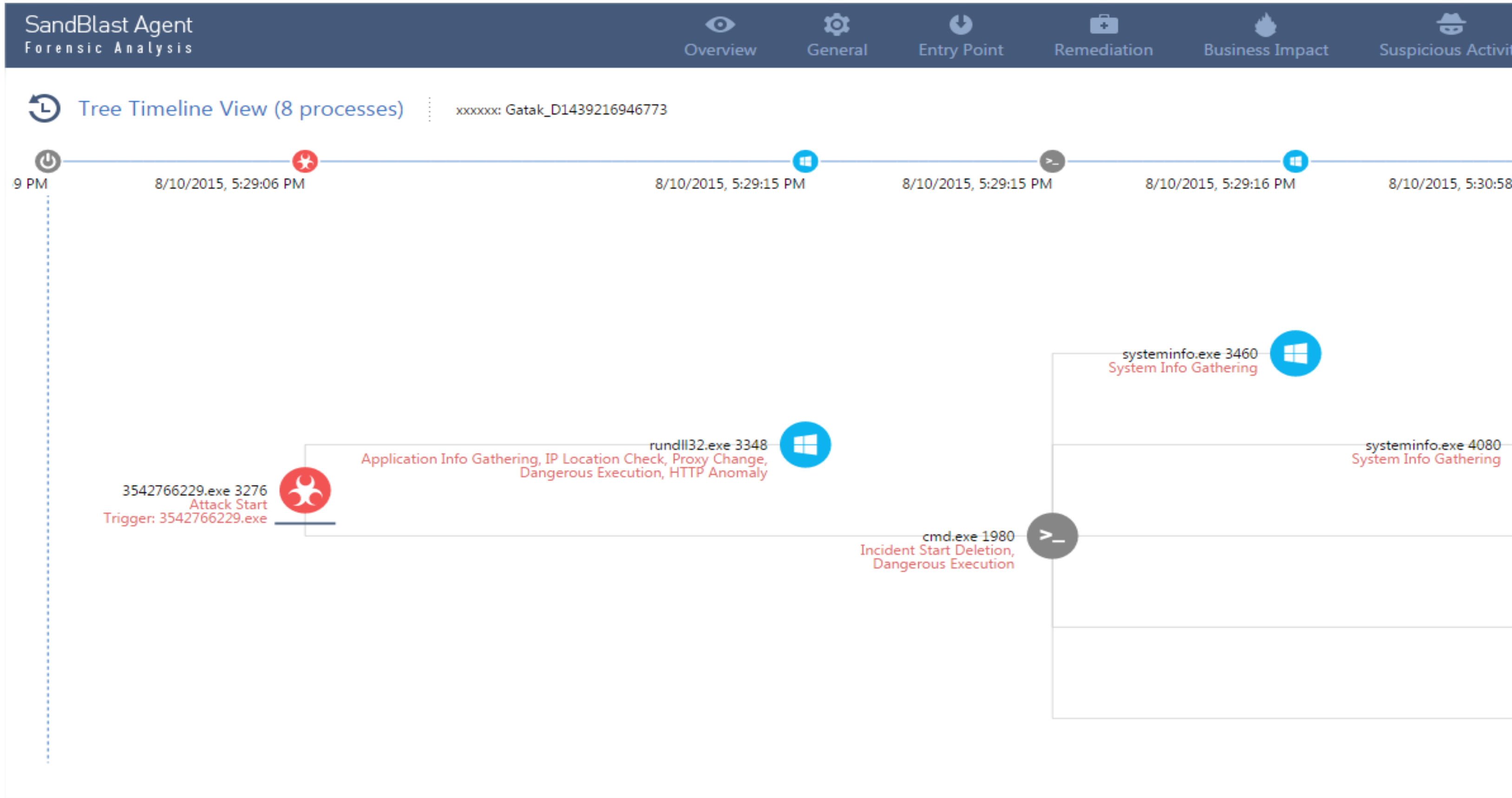
All Events (Last 200 events)

| Start Time | Event Name | Sever... | A... | P... | S... | Source | D... | Destination | Service | Attack Name | Attack Information | Verdict | User | Total num... | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 30 Jan 2015, 23:59 | Firewall | | | | | | | | 17 | | | | | | 9c2 |
| 30 Jan 2015, 23:58 | Firewall | | | | | | | | 17 | | | | | | a6d |
| 30 Jan 2015, 23:58 | IPS | | | | | 192.168.24.15 | | 10.82.114.7 | /80 | Web Server Enforcement Violation | ShellShock - GNU Bash Remote Code Execu... | | | | e70 |
| 30 Jan 2015, 23:57 | IPS | | | | | 192.168.24.15 | | 10.82.114.7 | /80 | Web Server Enforcement Violation | ShellShock - GNU Bash Remote Code Execu... | | | | e5c |
| 30 Jan 2015, 23:57 | Firewall | | | | | | | | 17 | | | | | | d82 |
| 30 Jan 2015, 23:49 | Firewall | | | | | | | | 17 | | | | | | 9c2 |
| 30 Jan 2015, 23:49 | IPS | | | | | 192.168.38.194 | | 10.38.193.100 | /80 | Web Server Enforcement Violation | ShellShock - GNU Bash Remote Code Execu... | | | | f55 |
| 30 Jan 2015, 23:46 | Firewall | | | | | | | | 17 | | | | | | 799 |
| 30 Jan 2015, 23:45 | Firewall | | | | | | | | 17 | | | | | | f8d |
| 30 Jan 2015, 23:44 | Firewall | | | | | | | | 17 | | | | | | 503 |
| 30 Jan 2015, 23:43 | Firewall | | | | | | | | 17 | | | | | | 640 |
| 30 Jan 2015, 23:43 | Firewall | | | | | | | | 17 | | | | | | f2f8 |
| 30 Jan 2015, 23:42 | Firewall | | | | | | | | 17 | | | | | | 3a1 |

3 Advanced algorithms analyze raw forensics data

WELCOME TO THE FUTURE OF CYBER SECURITY

# Forensic Analysis



Tree Timeline View (8 processes)

xxxxxx: Gatak_D1439216946773

3542766229.exe 3276
Attack Start
Trigger: 3542766229.exe

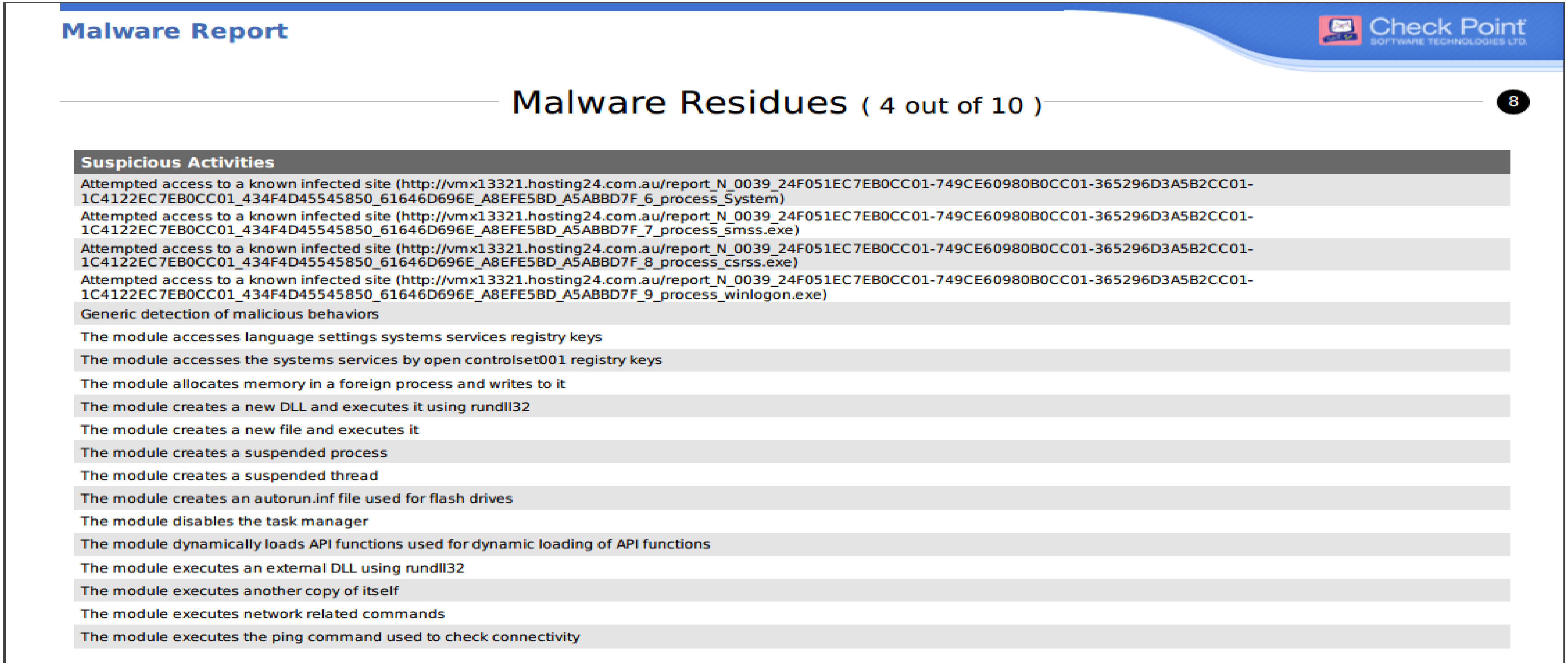
rundll32.exe 3348
Application Info Gathering, IP Location Check, Proxy Change, Dangerous Execution, HTTP Anomaly

cmd.exe 1980
Incident Start Deletion, Dangerous Execution

systeminfo.exe 3460
System Info Gathering

systeminfo.exe 4080
System Info Gathering

# Machine Learning



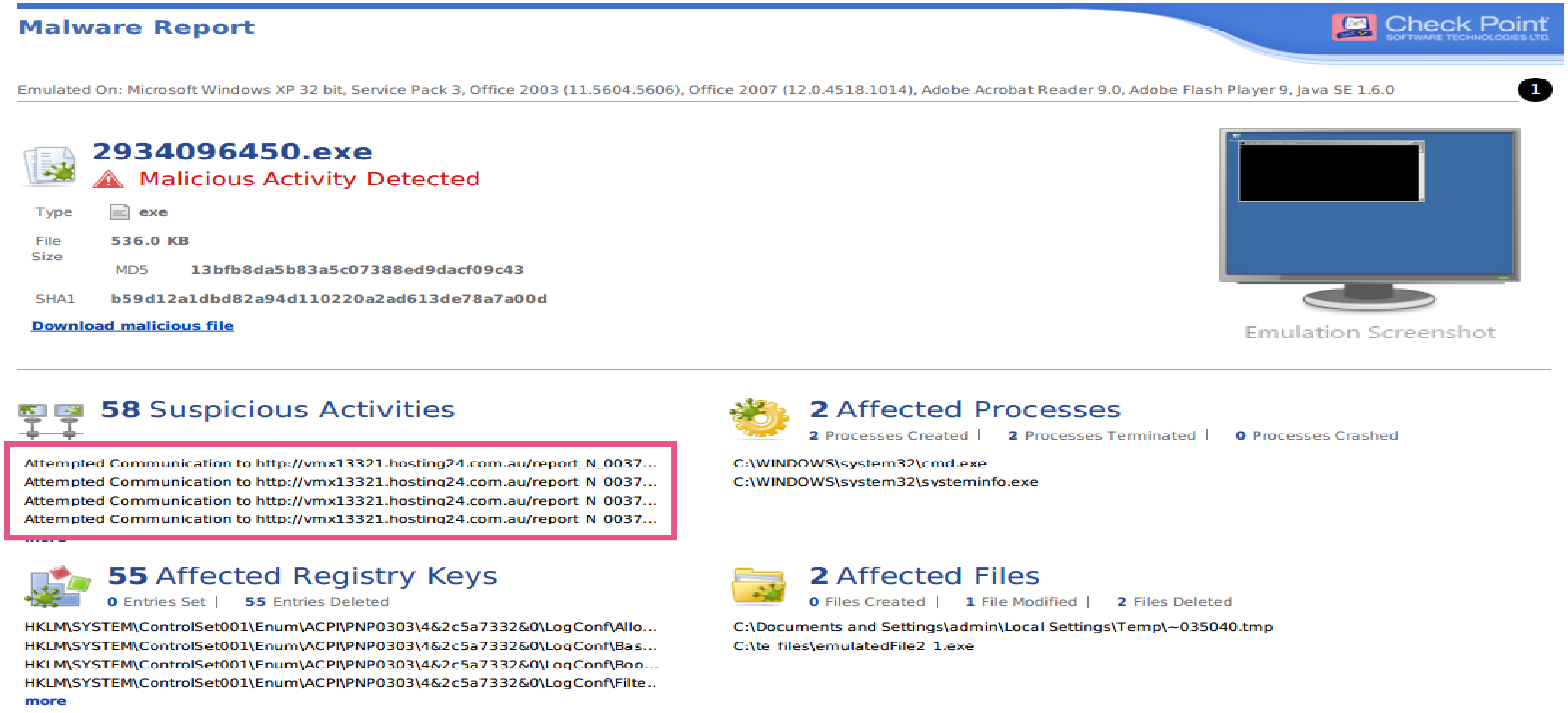
## Malware Report

### Malware Residues ( 4 out of 10 )

8

| Suspicious Activities |
|---|
| Attempted access to a known infected site (http://vmx13321.hosting24.com.au/report_N_0039_24F051EC7EB0CC01-749CE60980B0CC01-365296D3A5B2CC01-1C4122EC7EB0CC01_434F4D45545850_61646D696E_A8EFE5BD_A5ABBD7F_6_process_System) |
| Attempted access to a known infected site (http://vmx13321.hosting24.com.au/report_N_0039_24F051EC7EB0CC01-749CE60980B0CC01-365296D3A5B2CC01-1C4122EC7EB0CC01_434F4D45545850_61646D696E_A8EFE5BD_A5ABBD7F_7_process_smss.exe) |
| Attempted access to a known infected site (http://vmx13321.hosting24.com.au/report_N_0039_24F051EC7EB0CC01-749CE60980B0CC01-365296D3A5B2CC01-1C4122EC7EB0CC01_434F4D45545850_61646D696E_A8EFE5BD_A5ABBD7F_8_process_csrss.exe) |
| Attempted access to a known infected site (http://vmx13321.hosting24.com.au/report_N_0039_24F051EC7EB0CC01-749CE60980B0CC01-365296D3A5B2CC01-1C4122EC7EB0CC01_434F4D45545850_61646D696E_A8EFE5BD_A5ABBD7F_9_process_winlogon.exe) |
| Generic detection of malicious behaviors |
| The module accesses language settings systems services registry keys |
| The module accesses the systems services by open controlset001 registry keys |
| The module allocates memory in a foreign process and writes to it |
| The module creates a new DLL and executes it using rundll32 |
| The module creates a new file and executes it |
| The module creates a suspended process |
| The module creates a suspended thread |
| The module creates an autorun.inf file used for flash drives |
| The module disables the task manager |
| The module dynamically loads API functions used for dynamic loading of API functions |
| The module executes an external DLL using rundll32 |
| The module executes another copy of itself |
| The module executes network related commands |
| The module executes the ping command used to check connectivity |

# Polymorphic, but C2 is a giveaway



**Malware Report**

Emulated On: Microsoft Windows XP 32 bit, Service Pack 3, Office 2003 (11.5604.5606), Office 2007 (12.0.4518.1014), Adobe Acrobat Reader 9.0, Adobe Flash Player 9, Java SE 1.6.0

**2934096450.exe**

⚠ Malicious Activity Detected

Type: exe

File Size: 536.0 KB

MD5: 13bfb8da5b83a5c07388ed9dacf09c43

SHA1: b59d12a1dbd82a94d110220a2ad613de78a7a00d

Download malicious file

Emulation Screenshot

**58 Suspicious Activities**

Attempted Communication to http://vmx13321.hosting24.com.au/report_N_0037...
Attempted Communication to http://vmx13321.hosting24.com.au/report_N_0037...
Attempted Communication to http://vmx13321.hosting24.com.au/report N 0037...
Attempted Communication to http://vmx13321.hosting24.com.au/report N 0037...
more

**2 Affected Processes**

2 Processes Created | 2 Processes Terminated | 0 Processes Crashed

C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\systeminfo.exe

**55 Affected Registry Keys**

0 Entries Set | 55 Entries Deleted

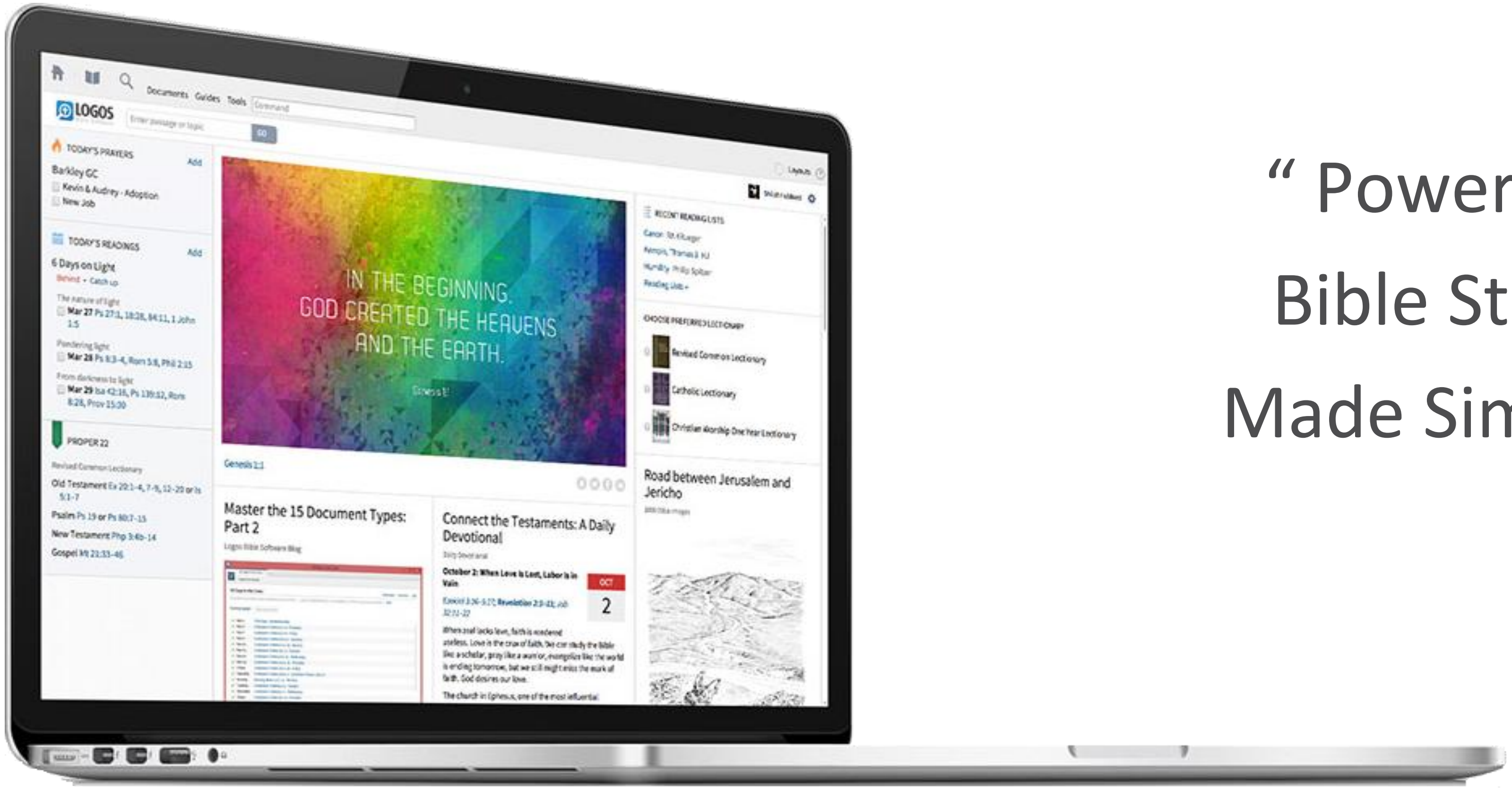
HKLM\SYSTEM\ControlSet001\Enum\ACPI\PNP0303\4&2c5a7332&0\LogConf\Allo...
HKLM\SYSTEM\ControlSet001\Enum\ACPI\PNP0303\4&2c5a7332&0\LogConf\Bas...
HKLM\SYSTEM\ControlSet001\Enum\ACPI\PNP0303\4&2c5a7332&0\LogConf\Boo...
HKLM\SYSTEM\ControlSet001\Enum\ACPI\PNP0303\4&2c5a7332&0\LogConf\Filte..
more

**2 Affected Files**

0 Files Created | 1 File Modified | 2 Files Deleted

C:\Documents and Settings\admin\Local Settings\Temp\~035040.tmp
C:\te files\emulatedFile2 1.exe

# In the beginning…

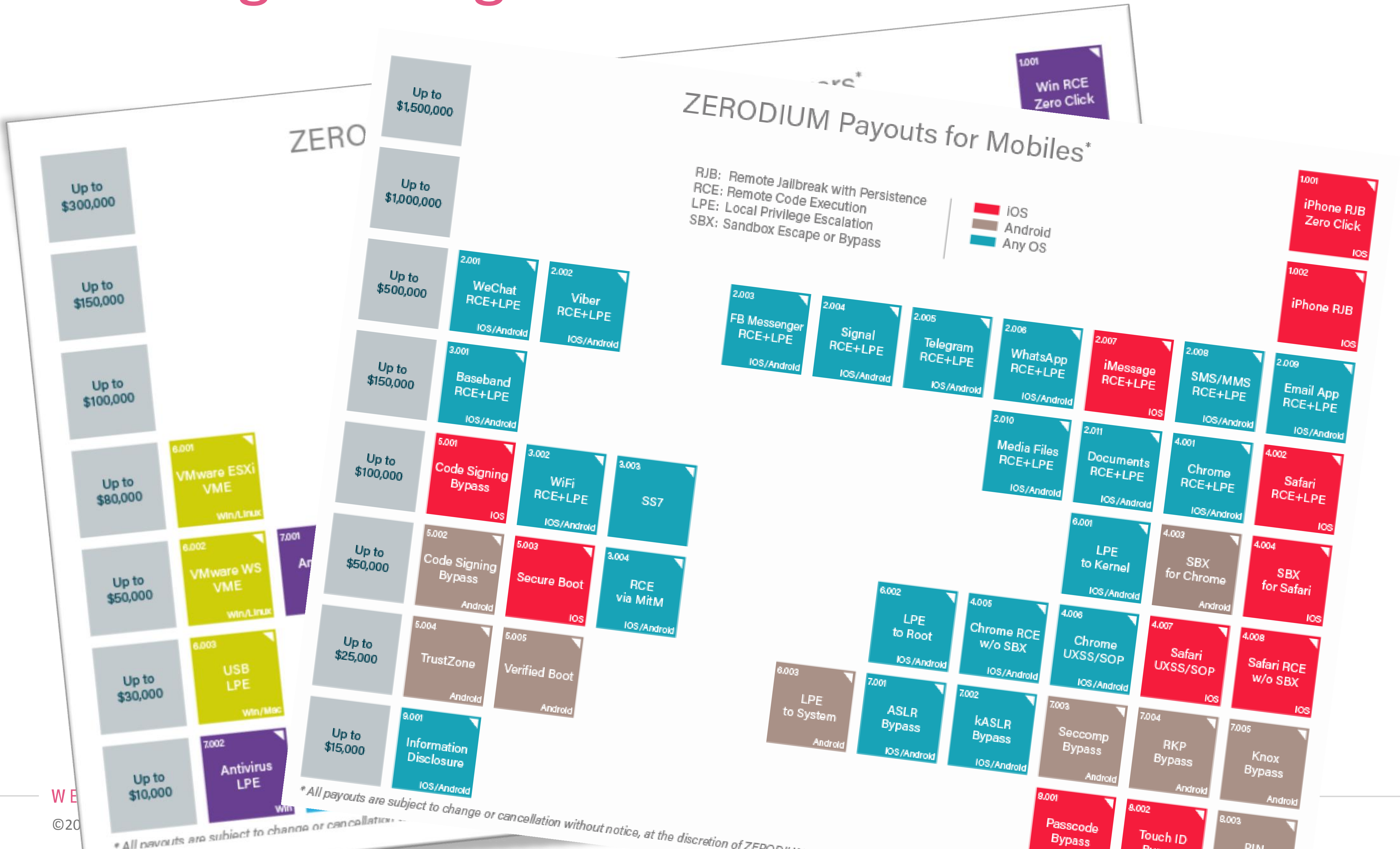

LOGOS
Documents
Guides
Tools
TODAY'S PRAYERS
Barkley GC
Kevin & Audrey - Adoption
New Job
TODAY'S READINGS
6 Days on Light
PROPER 22
Old Testament
Psalm
New Testament
Gospel
IN THE BEGINNING GOD CREATED THE HEAVENS AND THE EARTH.
Genesis 1:1
RECENT READING LISTS
CHOOSE PREFERRED LECTIONARY
Revised Common Lectionary
Catholic Lectionary
Christian Worship One Year Lectionary
Master the 15 Document Types: Part 2
Connect the Testaments: A Daily Devotional
OCT
2
Road between Jerusalem and Jericho

" Powerful

Bible Study

Made Simple! "

# Social Engineering is back



ZERO

…rs*

1.001 Win RCE Zero Click

Up to $300,000

Up to $150,000

Up to $100,000

Up to $80,000 — 6.001 VMware ESXi VME Win/Linux

Up to $50,000 — 6.002 VMware WS VME Win/Linux; 7.001 An…

Up to $30,000 — 6.003 USB LPE Win/Mac

Up to $10,000 — 7.002 Antivirus LPE Win

* All payouts are subject to change or cancellation…

## ZERODIUM Payouts for Mobiles*

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
▨ Android
🟦 Any OS

Up to $1,500,000 — 1.001 iPhone RJB Zero Click IOS

Up to $1,000,000 — 1.002 iPhone RJB IOS

Up to $500,000 — 2.001 WeChat RCE+LPE IOS/Android; 2.002 Viber RCE+LPE IOS/Android; 2.003 FB Messenger RCE+LPE IOS/Android; 2.004 Signal RCE+LPE IOS/Android; 2.005 Telegram RCE+LPE IOS/Android; 2.006 WhatsApp RCE+LPE IOS/Android; 2.007 iMessage RCE+LPE IOS; 2.008 SMS/MMS RCE+LPE IOS/Android; 2.009 Email App RCE+LPE IOS/Android

Up to $150,000 — 3.001 Baseband RCE+LPE IOS/Android; 2.010 Media Files RCE+LPE IOS/Android; 2.011 Documents RCE+LPE IOS/Android; 4.001 Chrome RCE+LPE IOS/Android; 4.002 Safari RCE+LPE IOS

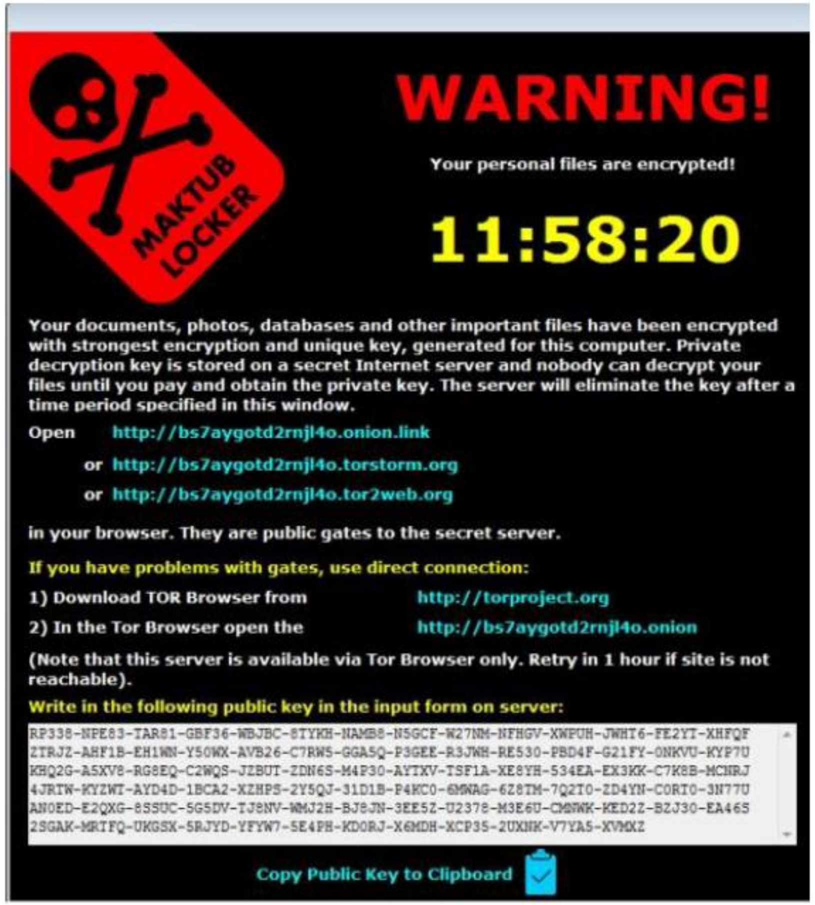
Up to $100,000 — 5.001 Code Signing Bypass IOS; 3.002 WiFi RCE+LPE IOS/Android; 3.003 SS7; 6.001 LPE to Kernel IOS/Android; 4.003 SBX for Chrome Android; 4.004 SBX for Safari IOS

Up to $50,000 — 5.002 Code Signing Bypass Android; 5.003 Secure Boot IOS; 3.004 RCE via MitM IOS/Android; 6.002 LPE to Root IOS/Android; 4.005 Chrome RCE w/o SBX IOS/Android; 4.006 Chrome UXSS/SOP IOS/Android; 4.007 Safari UXSS/SOP IOS; 4.008 Safari RCE w/o SBX IOS

Up to $25,000 — 5.004 TrustZone Android; 5.005 Verified Boot Android; 6.003 LPE to System Android; 7.001 ASLR Bypass IOS/Android; 7.002 kASLR Bypass IOS/Android; 7.003 Seccomp Bypass Android; 7.004 RKP Bypass Android; 7.005 Knox Bypass Android

Up to $15,000 — 9.001 Information Disclosure IOS/Android; 8.001 Passcode Bypass; 8.002 Touch ID B…; 8.003 PIN…

* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIU…



WARNING!

Your personal files are encrypted!

11:58:20

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://bs7aygotd2rnjl4o.onion.link

or http://bs7aygotd2rnjl4o.torstorm.org

or http://bs7aygotd2rnjl4o.tor2web.org

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1) Download TOR Browser from http://torproject.org

2) In the Tor Browser open the http://bs7aygotd2rnjl4o.onion

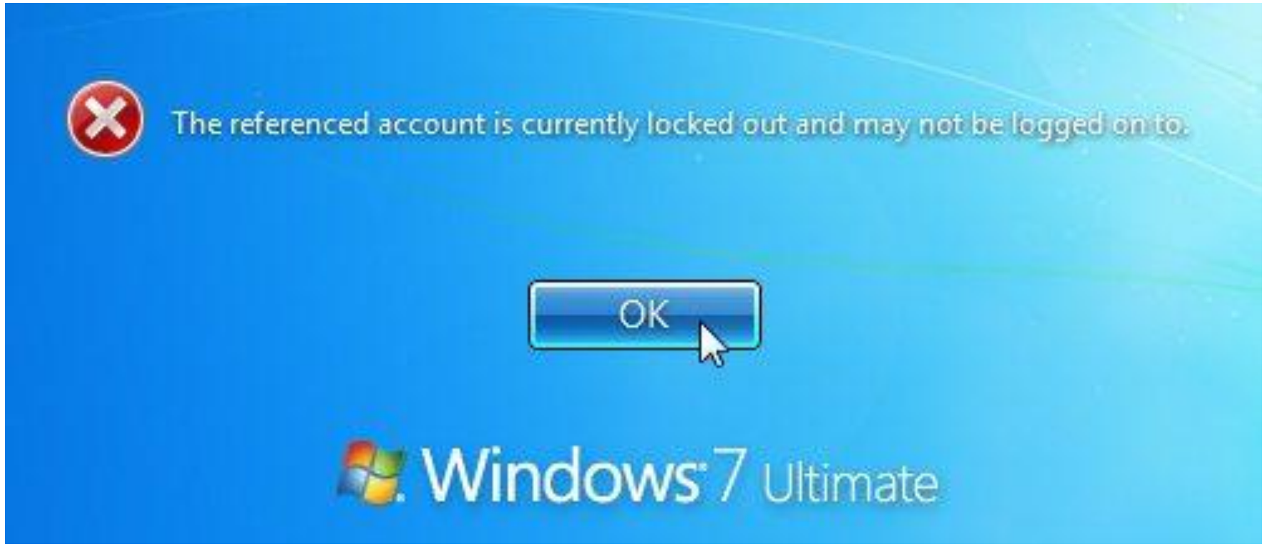
(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input form on server:

```
RP338-NPE83-TAR81-GBF36-WBJBC-8TYKH-NAMB8-N5GCF-W27NM-NFHGV-XWPUH-JWHT6-FE2YT-XHFQF
ZTRJZ-AHF1B-EH1WN-Y50WX-AVB26-C7RW5-GGA5Q-P3GEE-R3JWH-RE530-PBD4F-G21FY-0NKVU-KYP7U
KHQ2G-A5XV8-RG8EQ-C2WQS-JZBUT-ZDN6S-M4P30-AYTXV-TSF1A-XE8YH-534EA-EX3KK-C7K8B-MCNRJ
4JRTW-KYZWT-AYD4D-1BCA2-XZHPS-2Y5QJ-31D1B-P4KC0-6MWAG-6Z8TM-7Q2T0-ZD4YN-C0RT0-3N77U
AN0ED-E2QXG-8SSUC-5G5DV-TJ8NV-WMJ2H-BJ8JN-3EE5Z-U2378-M3E6U-CMNWK-KED2Z-BZJ30-EA465
2SGAK-MRTFQ-UKGSX-5RJYD-YFYW7-5E4PH-KD0RJ-X6MDH-XCP35-2UXNK-V7YA5-XVMXZ
```

Copy Public Key to Clipboard

## Let’s move everything to the cloud



The referenced account is currently locked out and may not be logged on to.

# Take Away

- Full gateway protections with controls that span all layers
- Account Take Over Protection
- Prevent!
  * (B) Ready to respond and remediate

# Ask us about

Check Point
SandBlast™
ZERO-DAY
PROTECTION

CHECK POINT
CloudGuard

Check Point
SOFTWARE TECHNOLOGIES LTD

# THANK YOU

Gad Naveh | Advanced Threat Prevention Evangelist

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION