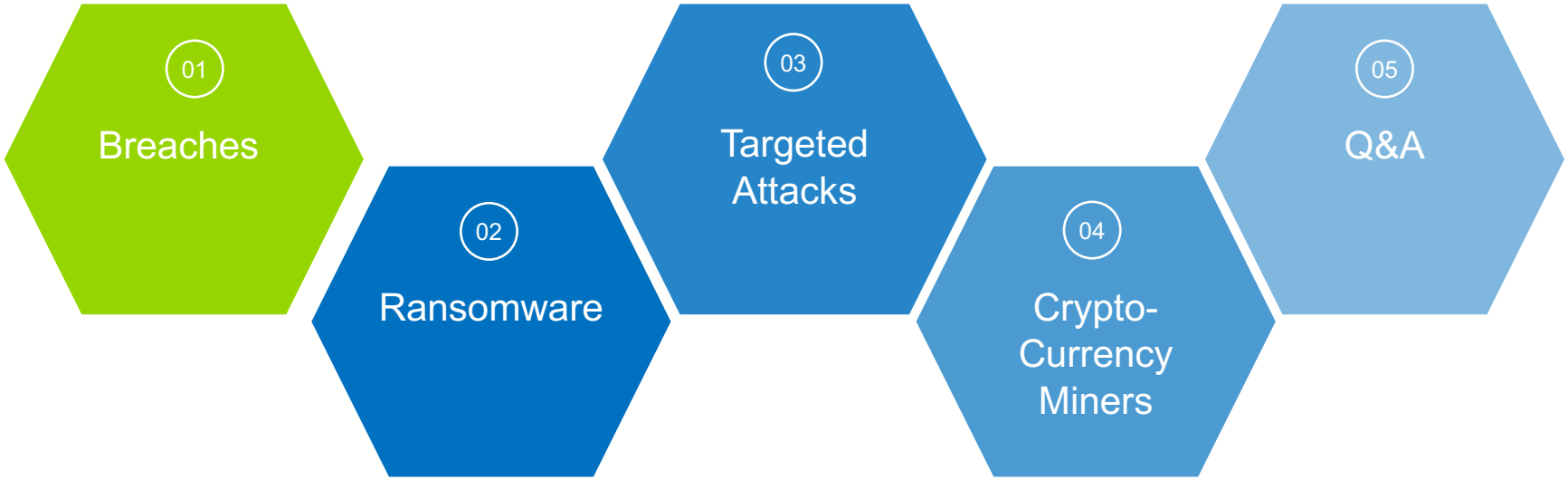
WEBROOT
Smarter Cybersecurity™

Tyler Moffitt
Senior Threat Research Analyst

Agenda



WEBROOT
Smarter Cybersecurity™

WEBROOT
Smarter Cybersecurity™

Breaches

Cybersecurity Attacks & Breaches Making News

By JONATHAN BERR / MONEYWATCH / September 7, 2017, 5:40 PM

Equifax breach exposed data for 143 million consumers

Equifax breach: Is it the biggest data breach?

TECHNOLOGY

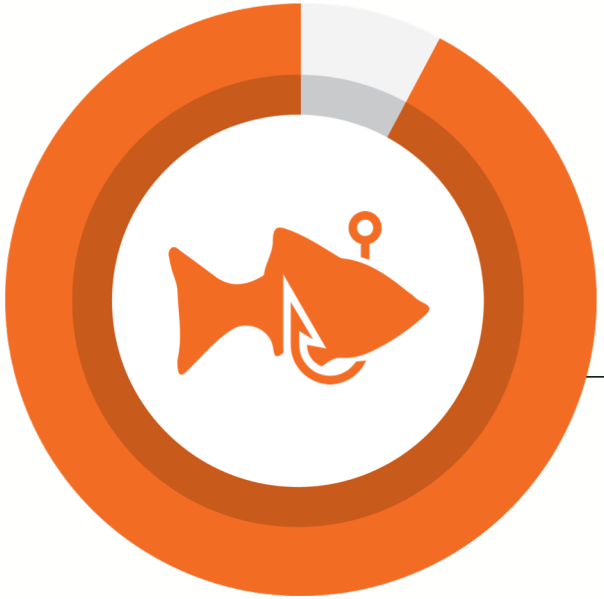
Yahoo Says 1 Billion User Accounts Were Hacked

NBC NEWS SECTIONS NIGHTLY NEWS MSNBC MEET THE PRESS DATELINE TODAY

SONY HACK

WEBROOT
Smarter Cybersecurity™

Risks for Users

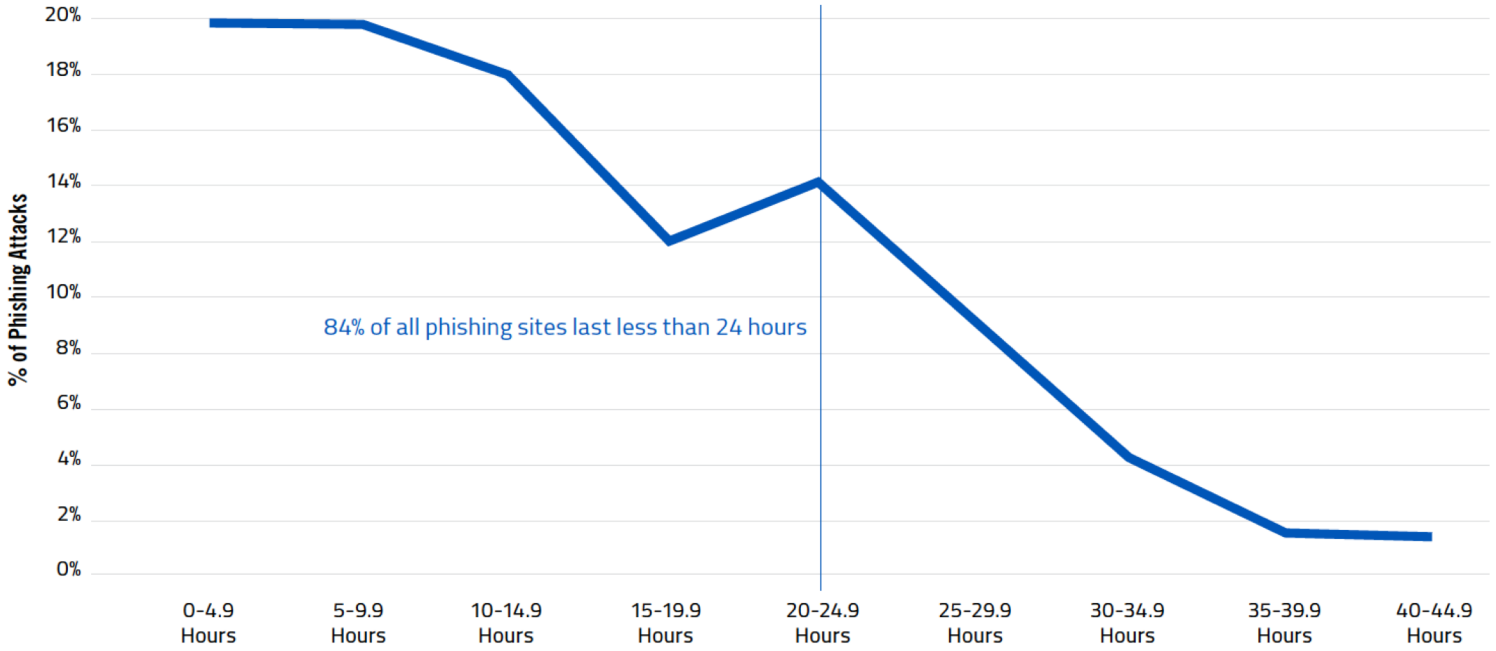


92%

chance of visiting a zero-day phishing site

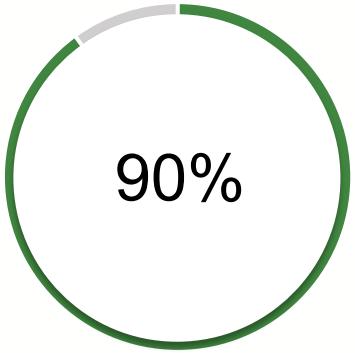
WEBROOT
Smarter Cybersecurity™

Attack Life Cycles are Getting Shorter

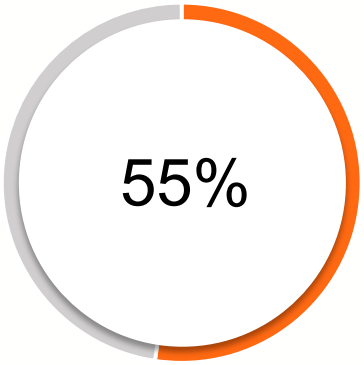


WEBROOT
Smarter Cybersecurity™

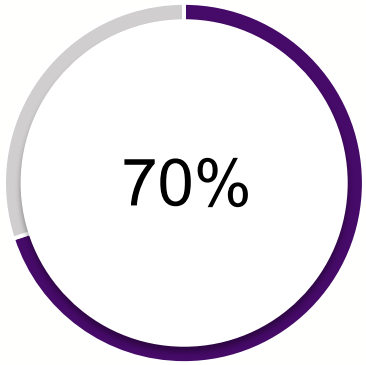
The High Cost of User Error



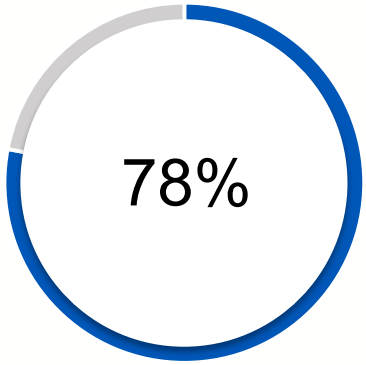
of successful data breaches caused by user error



of SMBs experienced a cyberattack in past year



of MSPs are not confident about stopping ransomware



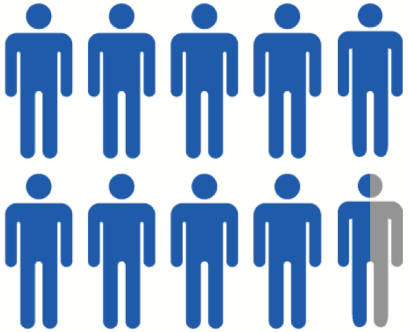
of MSPs encountered ransomware in past year

WEBROOT Smarter Cybersecurity™

User Error is a Big Issue

95%

of all successful cyber attacks is caused by human error



01 **Necessary:**
People are the weakest link in the security chain

02 **Proven:**
Educating employees can reduce security risk

03 **Best Practice:**
Security Awareness Training is a best practice or requirement for many industries

Source: IBM Cyber Security Intelligence Index

WEBROOT
Smarter Cybersecurity™

Webroot® Security Awareness Training Solution Overview

One centralized solution for ongoing awareness training

Phishing Simulator

- Raise awareness
- Test and **measure** end-users
- Integrated with training courses

Training Courses

- 40 course library including several **compliance** courses
- Easy administration
- One click user launch

Reporting/Compliance

- Integrated reporting center
- Meets compliance **requirements**

WEBROOT
Smarter Cybersecurity™

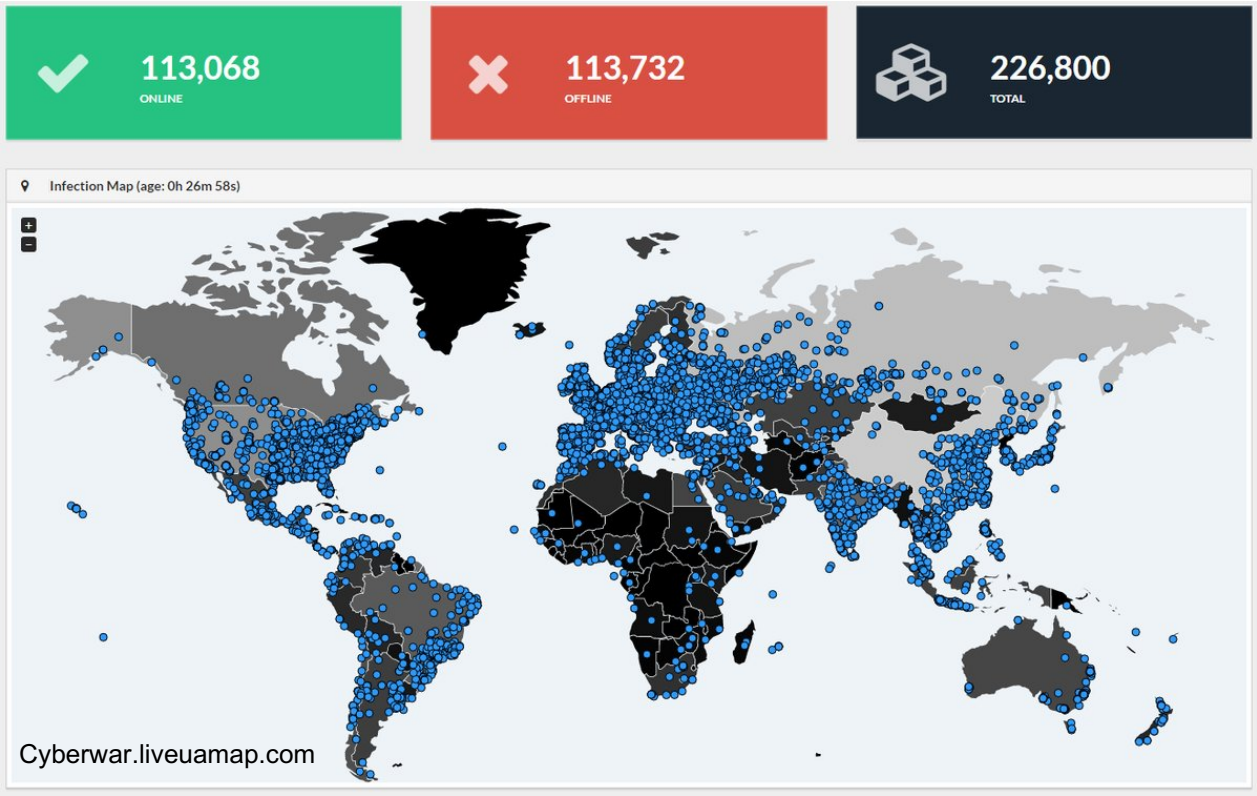
WEBROOT®
Smarter Cybersecurity™

Lateral Ransomware

WannaCrypt0r GUI

WEBROOT
Smarter Cybersecurity™

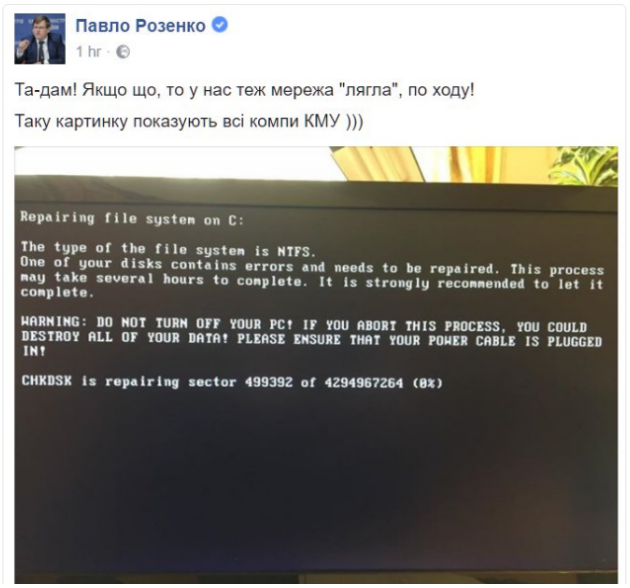
Record-Breaking Infection Count

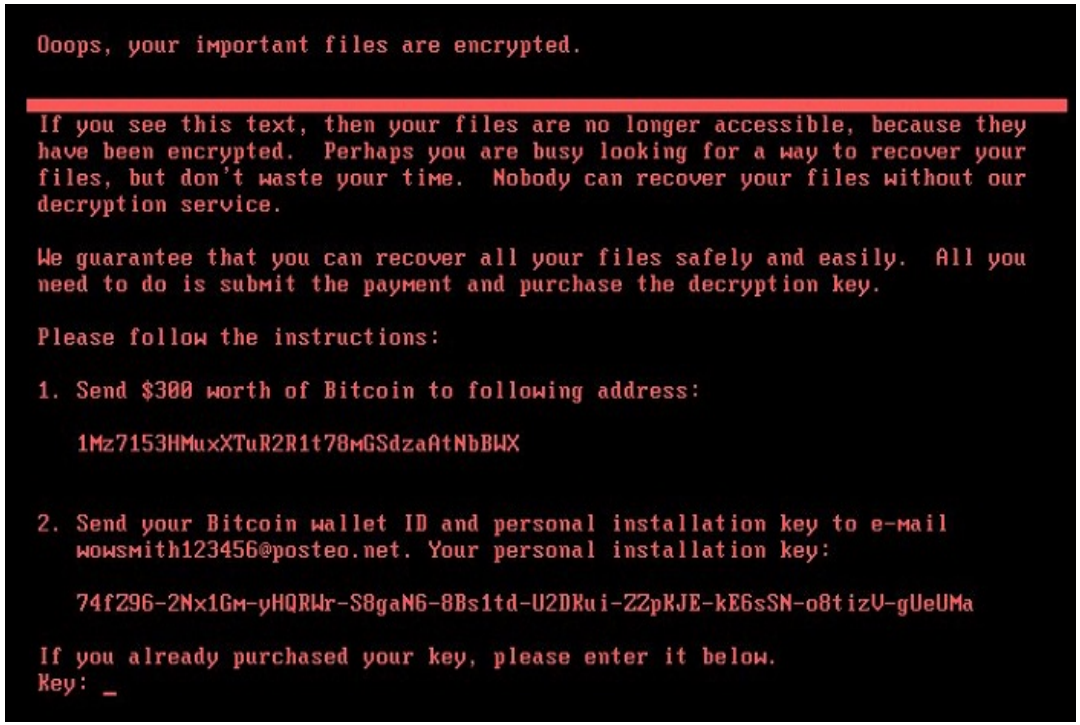


WEBROOT
Smarter Cybersecurity™

Not Petya: Encryption

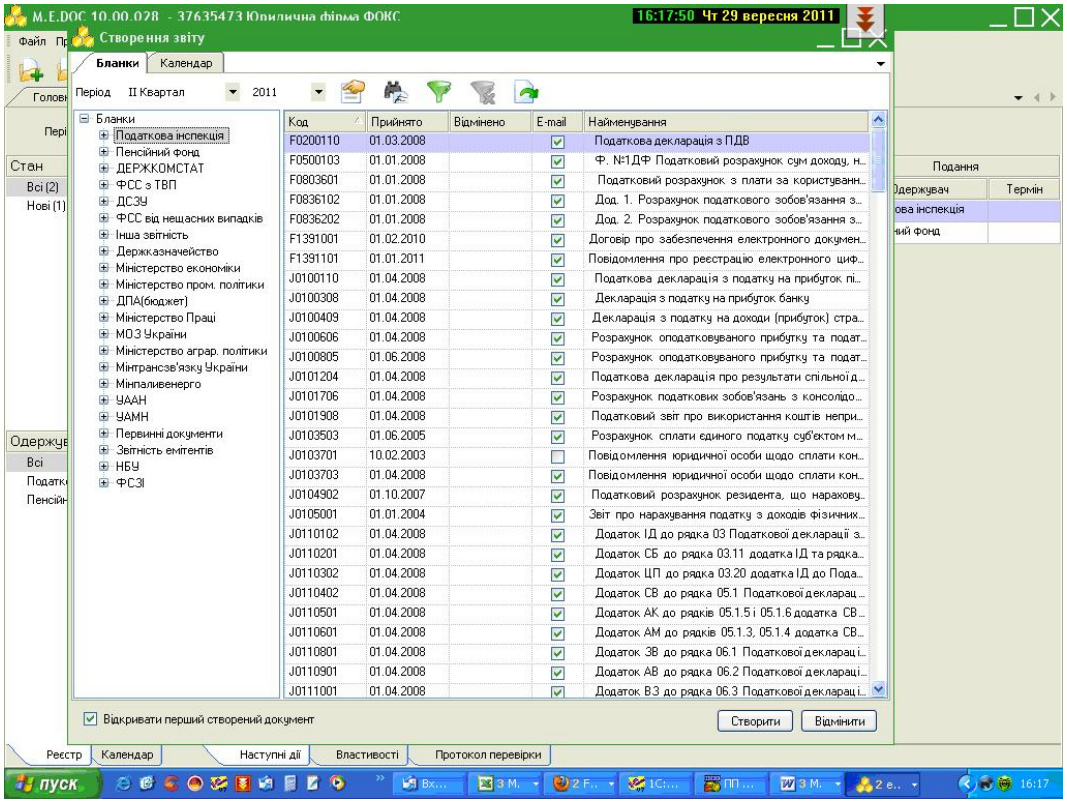
Vice Prime Minister of Ukraine, Павло Розенко (Pavlo Rozenko) on Facebook. This is what Petya looks like when it's encrypting your drive.





WEBROOT
Smarter Cybersecurity™

NotPetya Initial Vector – M.E. Doc Ukraine Tax Softare Update

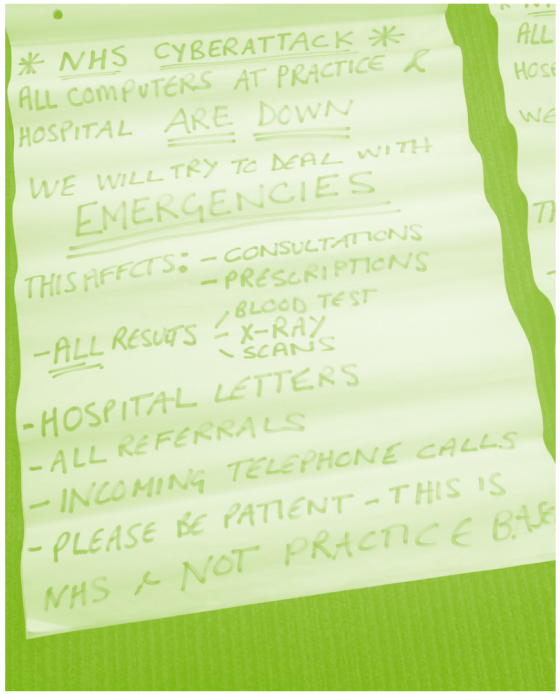


WEBROOT
Smarter Cybersecurity™

Similar Damage by NotPetya – Ukraine Focused

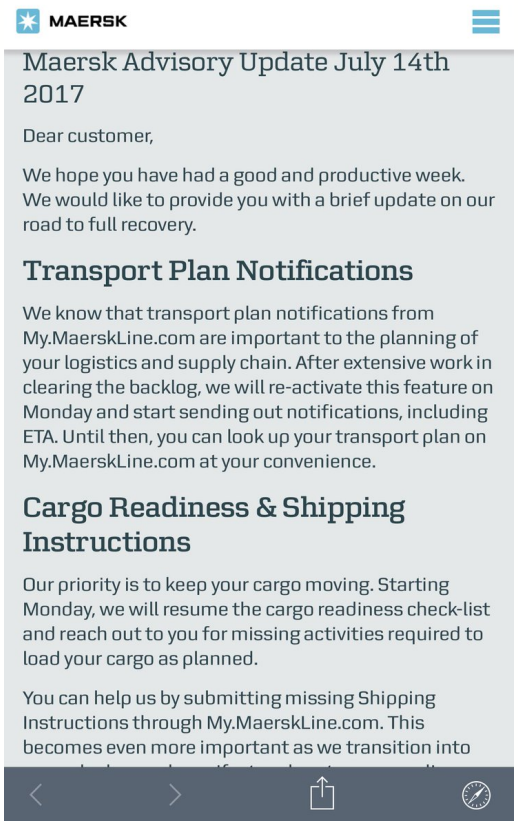
WEBROOT
Smarter Cybersecurity™

Many Organizations Shut Down by WannaCry & Not Petya



WEBROOT
Smarter Cybersecurity™

Major Corporation Still in Progress To Resume Full Operation



MAERSK

Maersk Advisory Update July 14th 2017

Dear customer,

We hope you have had a good and productive week. We would like to provide you with a brief update on our road to full recovery.

Transport Plan Notifications

We know that transport plan notifications from My.MaerskLine.com are important to the planning of your logistics and supply chain. After extensive work in clearing the backlog, we will re-activate this feature on Monday and start sending out notifications, including ETA. Until then, you can look up your transport plan on My.MaerskLine.com at your convenience.

Cargo Readiness & Shipping Instructions

Our priority is to keep your cargo moving. Starting Monday, we will resume the cargo readiness check-list and reach out to you for missing activities required to load your cargo as planned.

You can help us by submitting missing Shipping Instructions through My.MaerskLine.com. This becomes even more important as we transition into

MAERSK

FedEx Corporation

Reckitt Benckiser

WEBROOT Smarter Cybersecurity

Only a Couple Exploits Used From the Dump

- **EARLYSHOVEL** RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- **EBBISLAND (EBBSHAVE)** root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.
- **ECHOWRECKER** remote Samba 3.0.x Linux exploit.
- **EASYBEE** appears to be an MDaemon email server vulnerability
- **EASYPI** is an IBM Lotus Notes exploit that gets detected as Stuxnet
- **EWOKFRENZY** is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- **EXPLODINGCAN** is an IIS 6.0 exploit that creates a remote backdoor
- **ETERNALROMANCE** is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)
- **EDUCATEDSCHOLAR** is a SMB exploit (MS09-050)
- **EMERALDTHREAD** is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- **EMPHASISMINE** is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2
- **ENGLISHMANSDENTIST** sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users
- **EPICHERO** 0-day exploit (RCE) for Avaya Call Server
- **ERRATICGOPHER** is a SMBv1 exploit targeting Windows XP and Server 2003
- **ETERNALSYNERGY** is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)
- **ETERNALBLUE is** a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- **ETERNALCHAMPION** is a SMBv1 exploit
- **ESKIMOROLL** is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers
- **ESTEEMAUDIT** is an RDP exploit and backdoor for Windows Server 2003
- **ECLIPSEDWING** is an RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)
- **ETRE** is an exploit for IMail 8.10 to 8.22
- **FUZZBUNCH** is an exploit framework, similar to MetaSploit
- **ODDJOB** is an implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

Just some of the many exploits stolen in August 2016

01 The Equation Group are a CIA-affiliated hacking outfit

02 They owned a huge store of zero-day exploits

03 These exploits were stolen and are now being used to cause havoc

WEBROOT Smarter Cybersecurity™

Trends in Malware by Operating System

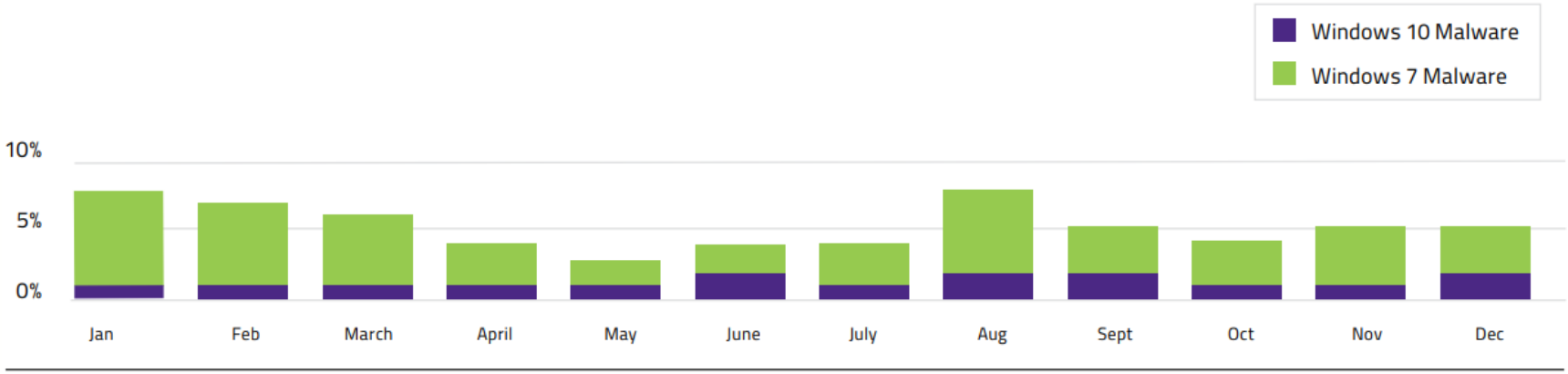


Figure 2: Malware on Windows 10 and Windows 7 devices by month, in 2017, as a percent of total malware seen across all operating systems

WEBROOT
Smarter Cybersecurity™

Targeted Attacks

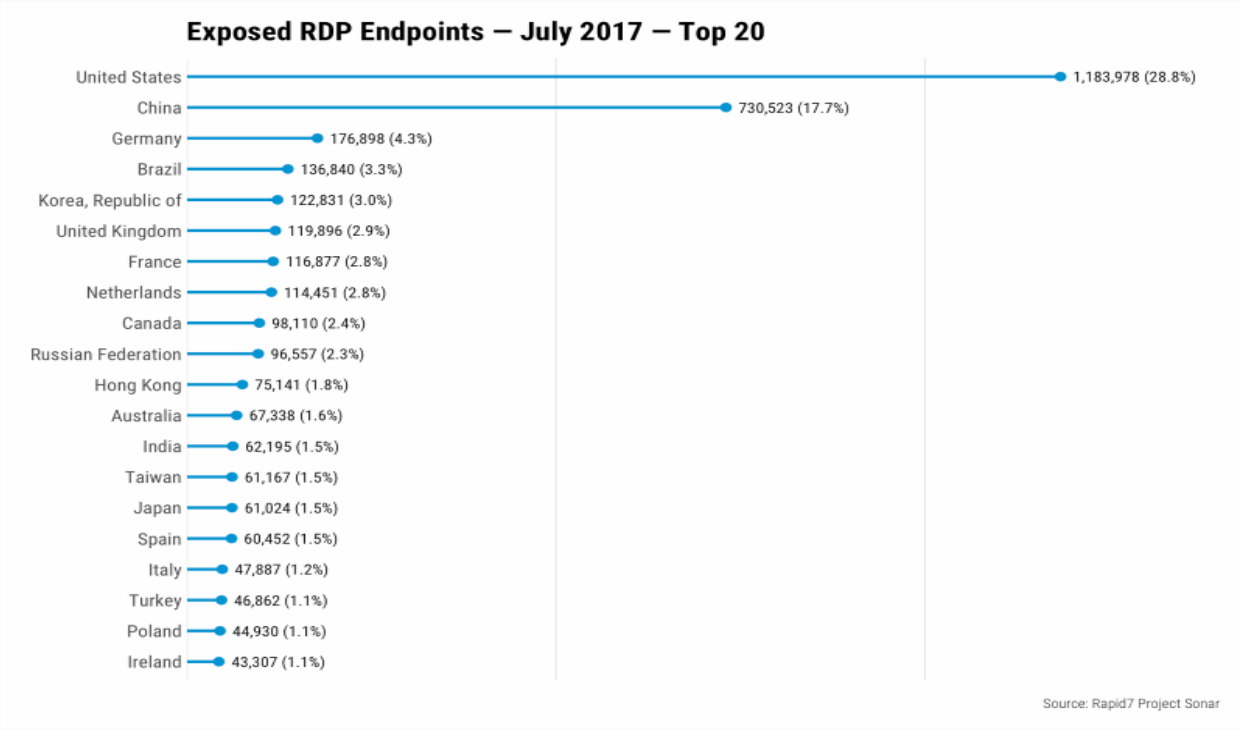
User Vulnerabilities

RDP Prevalence

Rapic7 bi-annual National Exposure Index scans

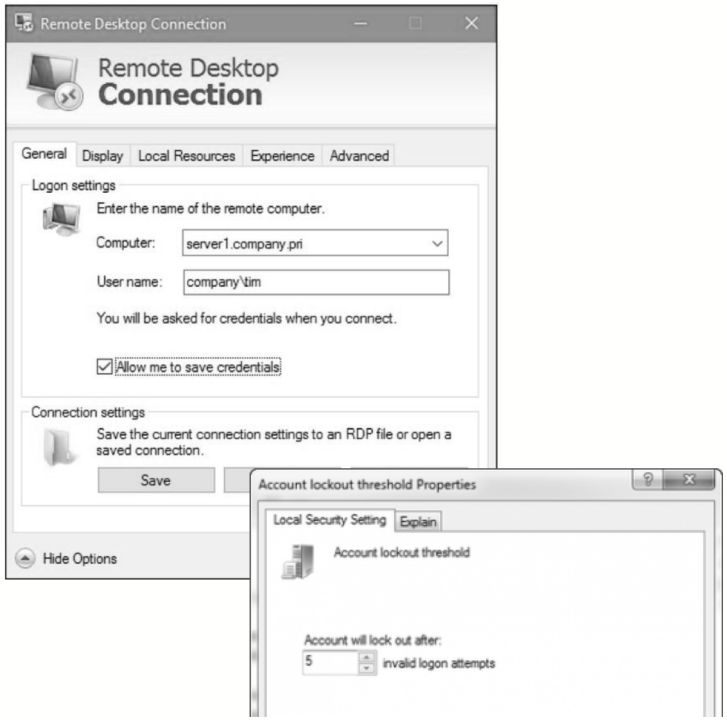
An internet-wide scan carried out by security researchers from Rapid7 had discovered over 11 million devices with 3389/TCP ports left open online, of which over 4.1 million are specifically speaking the RDP protocol.

A Webroot report from March 2017 pins RDP as the favorite method for delivering ransomware, topping spam campaigns.



WEBROOT
Smarter Cybersecurity™

RDP



RDP used by admins to control servers remotely

Gives hackers admin access to your whole network

The default port is easy to scan for by an attacker

Accounts can usually be cracked with brute force

https://www.webroot.com/blog/2016/11/23/remote-desktop-protocol-attacks-need-know/

WEBROOT
Smarter Cybersecurity™

Targeted Attacks – Killing the Weakest

BUSINESS

Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack

The SamSam ransomware variant has morphed into new mayhem, as dozens work around the clock to recover files

Atlanta Ransomware Attack Shows Cities Not Prepared for Long-Term Security Breaches

By John Bonazzo • 03/28/18 11:38am

NEWS

Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers

KIM ZETTER SECURITY 03.30.16 1:31 PM

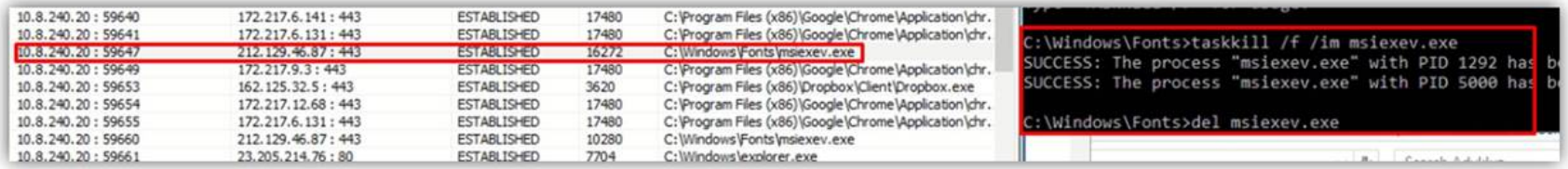
WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE

WEBROOT
Smarter Cybersecurity™

WEBROOT
Smarter Cybersecurity™

Cryptocurrency & Mining

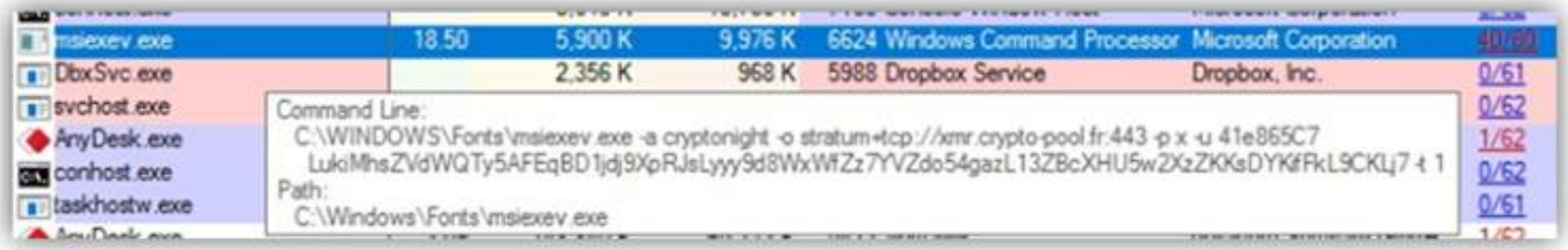
Miner Malware



10.8.240.20 : 59640	172.217.6.141 : 443	ESTABLISHED	17480	C:\Program Files (x86)\Google\Chrome\Application\chr.
10.8.240.20 : 59641	172.217.6.131 : 443	ESTABLISHED	17480	C:\Program Files (x86)\Google\Chrome\Application\chr.
10.8.240.20 : 59647	212.129.46.87 : 443	ESTABLISHED	16272	C:\Windows\Fonts\msiexev.exe
10.8.240.20 : 59649	172.217.9.3 : 443	ESTABLISHED	17480	C:\Program Files (x86)\Google\Chrome\Application\chr.
10.8.240.20 : 59653	162.125.32.5 : 443	ESTABLISHED	3620	C:\Program Files (x86)\Dropbox\Client\Dropbox.exe
10.8.240.20 : 59654	172.217.12.68 : 443	ESTABLISHED	17480	C:\Program Files (x86)\Google\Chrome\Application\chr.
10.8.240.20 : 59655	172.217.6.131 : 443	ESTABLISHED	17480	C:\Program Files (x86)\Google\Chrome\Application\chr.
10.8.240.20 : 59660	212.129.46.87 : 443	ESTABLISHED	10280	C:\Windows\Fonts\msiexev.exe
10.8.240.20 : 59661	23.205.214.76 : 80	ESTABLISHED	7704	C:\Windows\explorer.exe

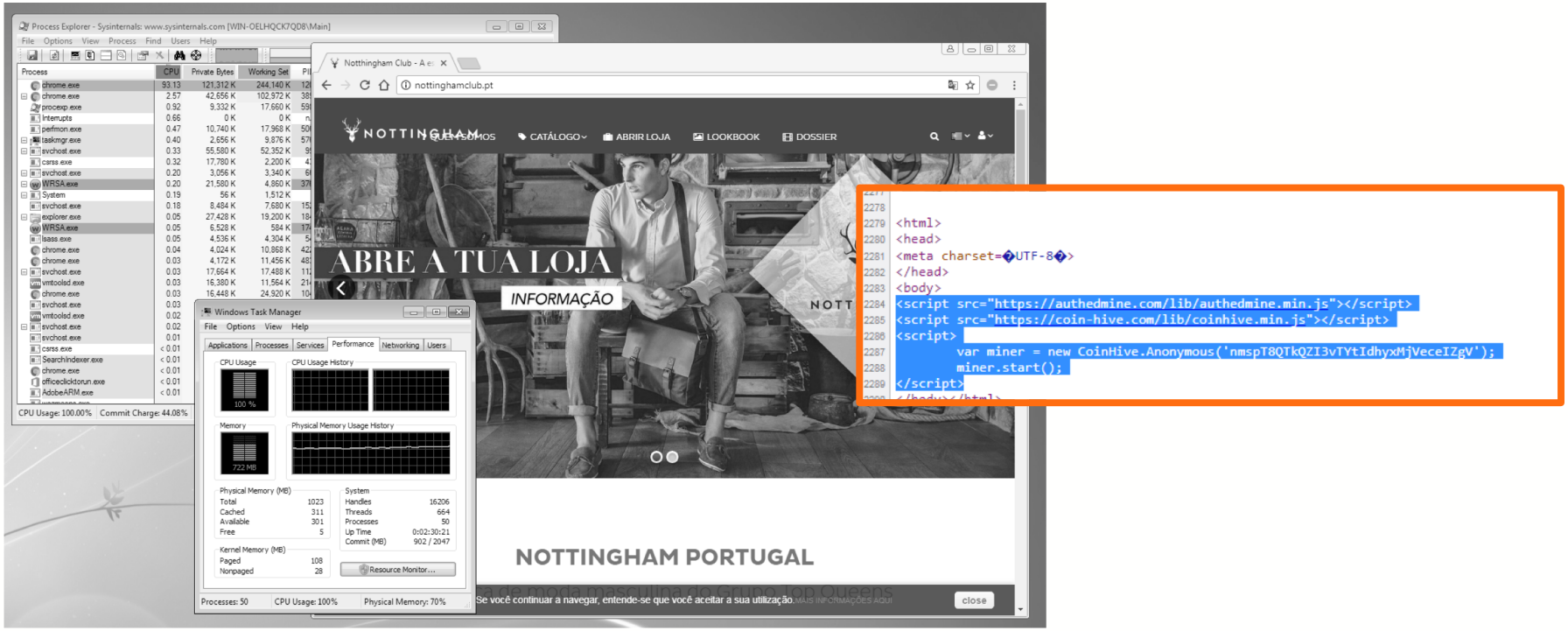
```
C:\Windows\Fonts>taskkill /f /im msiexev.exe
SUCCESS: The process "msiexev.exe" with PID 1292 has b
SUCCESS: The process "msiexev.exe" with PID 5000 has b

C:\Windows\Fonts>del msiexev.exe
```



15 May 2017: I repeat botnets not accepted
15 April 2017: For test I have reduce minimal threshold (5 to 2 XMR Exchange or 0.5 to 0.3XMR wallet)
26 January 2017: For mining with exchange use ADDRESS.PAYMENTID for mining and website.
14 January 2017: Website/Api/Mining is in https (Port 8443 for GPU Claymore SSL).
08 January 2017: Choice your DIFF with YOUR_WALLET_ADDRESS+DIFF on username.

The Emergence of CryptoJacking



WEBROOT
Smarter Cybersecurity™

WEBROOT
Smarter Cybersecurity™

Questions?

Tyler Moffitt
tmoffitt@webroot.com