

Event Viewer									
File Action View Help									
Event Viewer (Local)									
Application 2,603 event(s)									
Application	Type	Date	Time	Source	Category	Event	User	Computer	
Security	Information	24/01/2012	14:57:11	gupdate	None	0	N/A	UK-GN-20241	
System	Information	24/01/2012	14:55:00	gupdate	None	0	N/A	UK-GN-20241	
Cisco AnyConnect VPN Client	Information	24/01/2012	13:57:17	gupdate	None	0	N/A	UK-GN-20241	
Microsoft Office Diagnostics	Information	24/01/2012	13:55:02	gupdate	None	0	N/A	UK-GN-20241	
Microsoft Office Sessions	Information	24/01/2012	10:53:37	SecCl	None	1704	N/A	UK-GN-20241	
	Information	24/01/2012	09:31:33	Outlook	None	32	N/A	UK-GN-20241	
	Information	24/01/2012	09:05:51	Outlook	None	26	N/A	UK-GN-20241	
	Information	24/01/2012	09:05:48	Outlook	None	26	N/A	UK-GN-20241	
	Error	24/01/2012	09:05:13	Userenv	None	1030	SYSTEM	UK-GN-20241	
	Error	24/01/2012	09:05:13	Userenv	None	1058	SYSTEM	UK-GN-20241	
	Information	24/01/2012	08:55:03	gupdate	None	0	N/A	UK-GN-20241	
	Information	24/01/2012	08:55:01	gupdate	None	0	N/A	UK-GN-20241	
	Error	24/01/2012	08:45:35	Sophos Message Router	Runtime ...	8005	SYSTEM	UK-GN-20241	
	Warning	24/01/2012	08:45:32	Sophos Message Router	Runtime ...	8004	SYSTEM	UK-GN-20241	
	Error	24/01/2012	08:44:48	AutoEnrollment	None	15	N/A	UK-GN-20241	
	Error	24/01/2012	08:43:36	Userenv	None	1054	SYSTEM	UK-GN-20241	
	Information	24/01/2012	08:40:34	Windows Search Service	Search s...	1003	N/A	UK-GN-20241	
	Information	24/01/2012	08:40:30	SecurityCenter	None	1807	N/A	UK-GN-20241	
	Information	24/01/2012	08:40:23	ESENT	General	102	N/A	UK-GN-20241	
	Information	24/01/2012	08:40:23	ESENT	General	100	N/A	UK-GN-20241	
	Information	24/01/2012	08:40:16	TOSHIBA Bluetooth Se...	None	0	N/A	UK-GN-20241	
	Warning	24/01/2012	08:40:11	EvrkAgnit	None	1015	N/A	UK-GN-20241	
	Warning	24/01/2012	08:40:11	EvrkAgnit	None	1003	N/A	UK-GN-20241	
	Error	24/01/2012	08:40:10	AutoEnrollment	None	15	N/A	UK-GN-20241	
	Error	24/01/2012	08:40:10	Userenv	None	1054	SYSTEM	UK-GN-20241	
	Information	24/01/2012	08:40:03	gupdate	None	0	N/A	UK-GN-20241	
	Warning	23/01/2012	17:24:48	Userenv	None	1517	SYSTEM	UK-GN-20241	
	Information	23/01/2012	16:57:14	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	16:55:02	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	15:57:10	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	15:55:00	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	14:57:14	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	14:55:01	gupdate	None	0	N/A	UK-GN-20241	
	Error	23/01/2012	13:57:23	Userenv	None	1054	SYSTEM	UK-GN-20241	
	Information	23/01/2012	13:57:15	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	13:55:00	gupdate	None	0	N/A	UK-GN-20241	
	Information	23/01/2012	10:47:14	SecCl	None	1704	N/A	UK-GN-20241	
	Information	23/01/2012	09:19:01	Outlook	None	32	N/A	UK-GN-20241	
	Error	23/01/2012	09:08:45	Userenv	None	1030	SYSTEM	UK-GN-20241	
	Error	23/01/2012	09:08:45	Userenv	None	1058	SYSTEM	UK-GN-20241	
	Information	23/01/2012	09:08:00	Outlook	None	30	N/A	UK-GN-20241	
	Error	23/01/2012	09:02:21	AutoEnrollment	None	15	N/A	UK-GN-20241	

Shortcut to
Internet

Shortcut to
E-mail

MSN Installer



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

OK Cancel Browse...



avg_free_st...



Recycle Bin

start

Hotmail, Messenger, ...

EN 13:46



Advanced WindowsCare V2 Personal

Advanced WindowsCare 2 Personal

Restore Center Tools Options

Operation System: Microsoft Windows XP

Processor Info: AMD Athlon(tm) 64 X2 Dual Core Proces...

Video Device:

Physical Memory: 511MB

[Details...](#)

☒ **Spyware Removal**
Scan and remove Spyware and Adware. **16 problems found.**
[Show details...](#)

☒ **Security Defense**
Prevent Spyware from being installed in your PC. **32390 items unprotected.**
[Show details...](#)

☒ **Registry Fix**
Fix invalid or incorrect registry entries and values. **40 problems found.**
[Show details...](#)

☒ **System Optimization**
Optimize and repair system configuration. **84 problems found.**
[Show details...](#)

☒ **Startup Manage**
Control and optimize Windows startup items. **1 item found.**
[Show details...](#)

☒ **Privacy Sweep**
Erase your activity history and surfing traces. **9 problems found.**
[Show details...](#)

☒ **Junk Files Clean**
Clean up junk files and recover disk space. **36MB files found.**
[Show details...](#)

☒ **Need More Windows Care Services?**

[UpgradeNow!](#)

[Status](#) [Repair](#) [Close](#)



Virtual Payment Terminal

Purchase Details

* Transaction Type

PC Support and Optimization

* Description

Platinum Plan

* Currency

☐ USD ☒ GBP ☐ AUD ☐ CAD

* Amount

89 ~ ₹8000

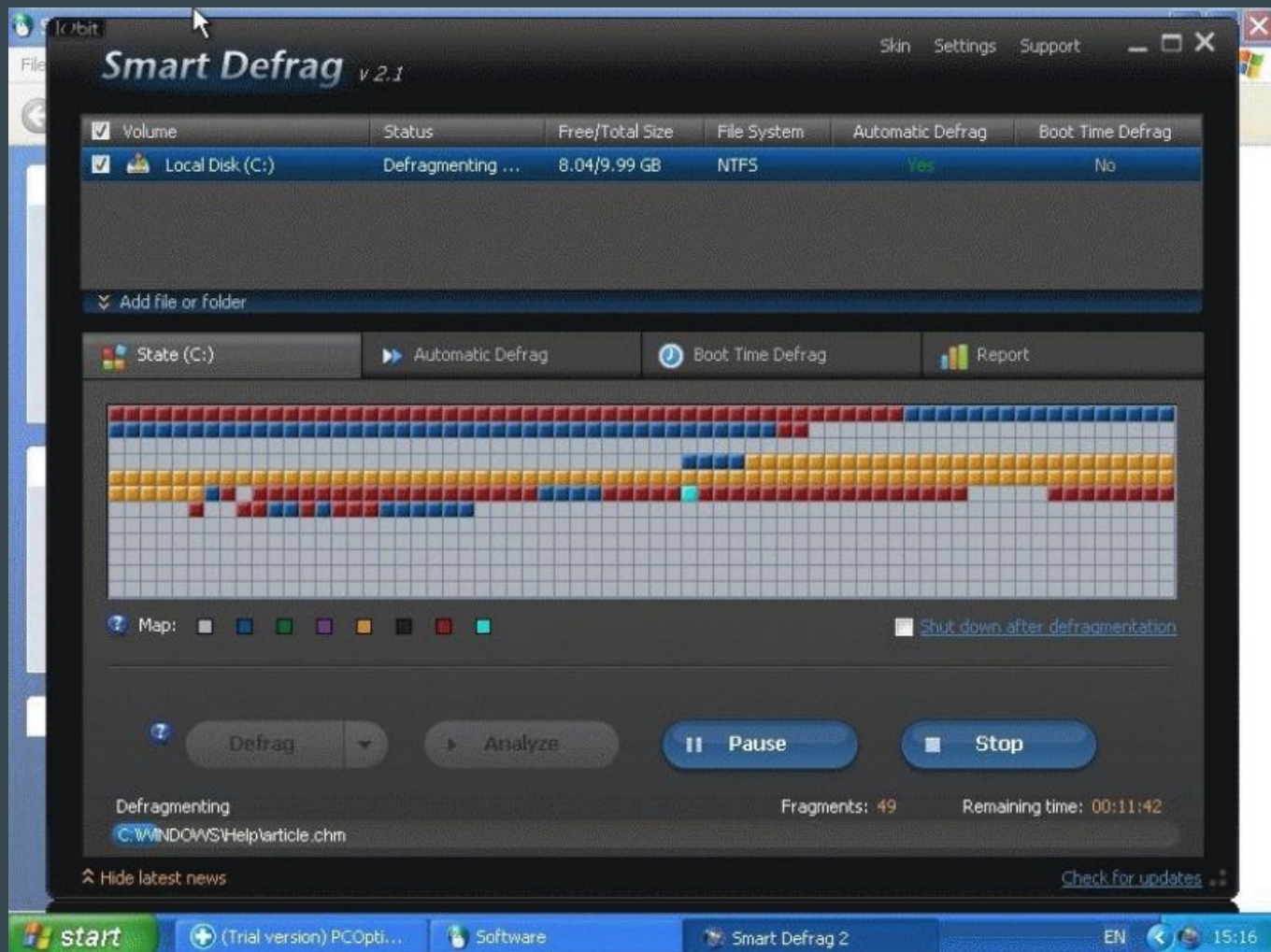
Credit Card Details

* Card Number

* CARD TYPE

* Card Holder Name

type as printed on the card



- Shortcut to Internet
- Shortcut to E-mail
- MSN Installer
- AMMY
- Smart Defrag 2
- Software
- McAfee Security Sc...

 **McAfee**
An Intel Company

Security Scan Plus

Home | Settings | Help

 **Your PC is at risk.**

About McAfee | Scan again

Virus and Spyware Protection

! Not found

We did not find any virus protection product on your PC. Don't leave your PC defenseless against the latest threats.

[Get McAfee protection.](#)

Firewall Protection

✓ On

McAfee Web Protection

! Not found

Threats Detection

✓ None

At Risk

Your PC is At Risk

About McAfee

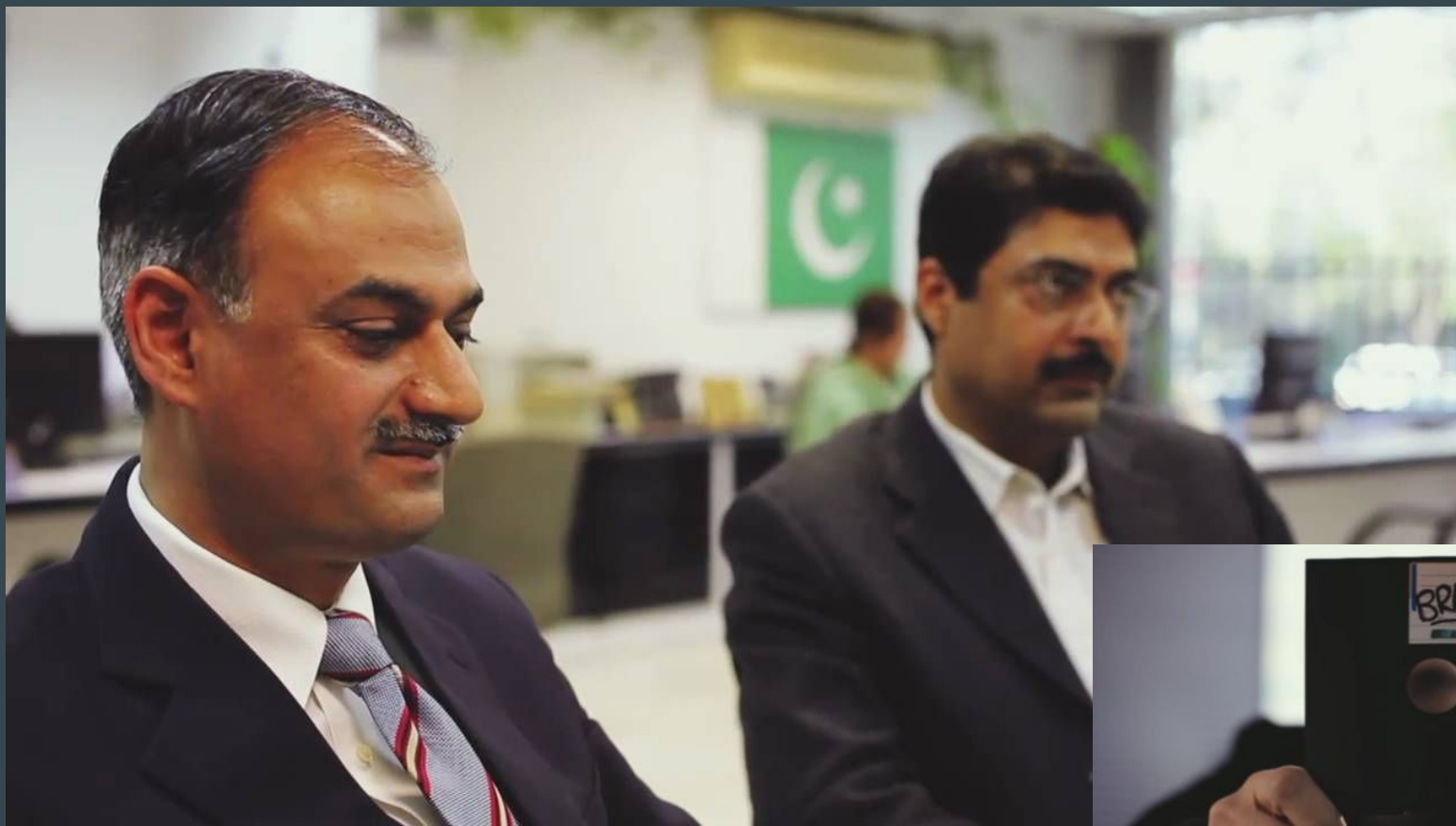
j_free_st...



The state of Malware from the Eye of the Tiger

...

Martijn Grooten, Virus Bulletin
Nullcon, Goa, March 2019



Source: F-Secure

About me

@martijn_grooten

Virus Bulletin

I am not a reverse engineer

I have never done security 'in the real world'

I have never been to Black Hat or Defcon

I am a mathematician, but never finished my PhD

I believe in facing the imposter syndrome head-on

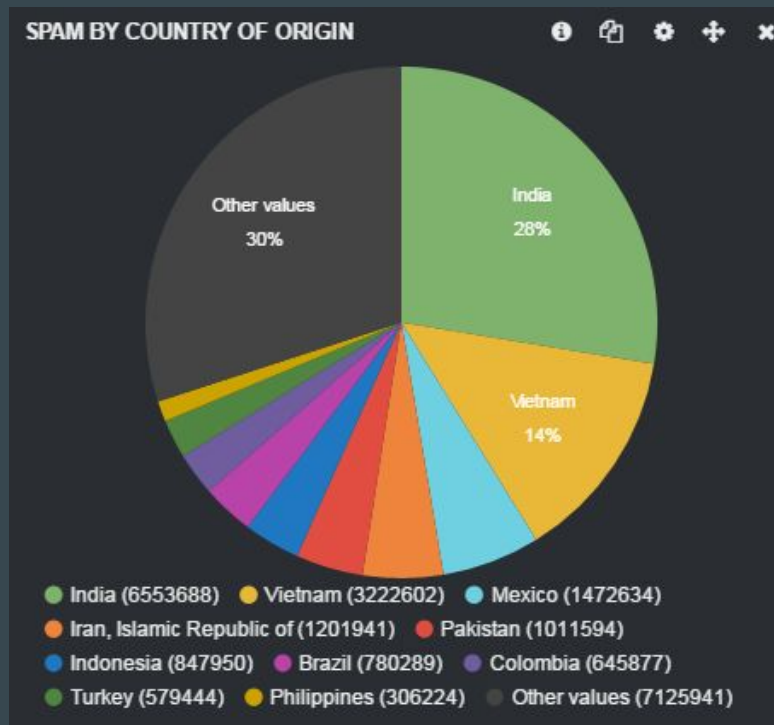
Phone support scams

Lessons learned

Social engineering is effective

Don't ignore economy when focusing
on cybercrime

Necurs



Source: Trustwave

Necurs has not actively spread for years

From Adolfo Lodge <[REDACTED]> ☆

Reply

Reply All ▾

Forward

More ▾

Subject **This crypto coin could go up fifty thousand percent this year**

13/01/18 19:33

To [REDACTED] ☆

Dear [REDACTED],

If you don't already own a few coins of something, then surely at the very least, you must have heard about cryptocurrencies.

Bitcoin, the most famous one, minted countless multimillionaires but did you know that altcoins (bitcoin alternatives) are responsible for even more riches?

Among the "big" ones, NEM went up almost 10,000 percent and Ethereum, more than 4,000 percent

Among the small and unknown ones several gained more than 50,000 percent.

To put this in perspective, a small 1,000-dollar coin purchase in one of these small ones could have turned into more than 50 million bucks.

It seems crazy, doesn't it? Well, it's the reality of the cryptocurrency market today.

Raiblocks, a relatively obscure coin at the time, went from 0.20 on December first to \$20 by New Year's Eve. It is now in the top 20 largest coins in the world.

All that to say, the next big winner could be found anywhere, and today I believe I've identified the next one.

After spending hundreds of hours looking at hundreds of different coins, I locked down on one specific target.

‘Dumb’ things to do with a botnet

Spamming

DDoS

Cryptocurrency mining

Proxy network

Necurs getting smart

2. **Bots that are under or able to reach bank-related domains.**^[2] The modules execute commands such as “net view” and “net user” to check for the following strings:

- BANQ
- BANK
- BANC
- SWIFT
- BITCOIN
- WESTERNUNION
- MONEYGRAM
- CARD

Source: Trend Micro

Necurs

Lessons learned

Dumb botnets focus on quantity rather than quality

Typical infections are poorly secured devices (old/unlicensed Windows, IoT, etc)

Even dumb botnets have smart parts

Emotet

“We have detected 5,000 spam emails everyday carrying Trojans targeting businesses and individuals in the last one month. From Trojan to Complex Threat Distributor, more than 1.5 lakh incidents related to the Emotet Trojan have been reported in the last one month,” Sanjay Katkar, Joint Managing Director and Chief Technology Officer, Quick Heal Technologies, said.

Source: The Hindu Business Line

2014: just another banking trojan

New Banking Malware Uses Network Sniffing for Data Theft

Posted on: June 27, 2014 at 8:47 am Posted in: Malware, Spam

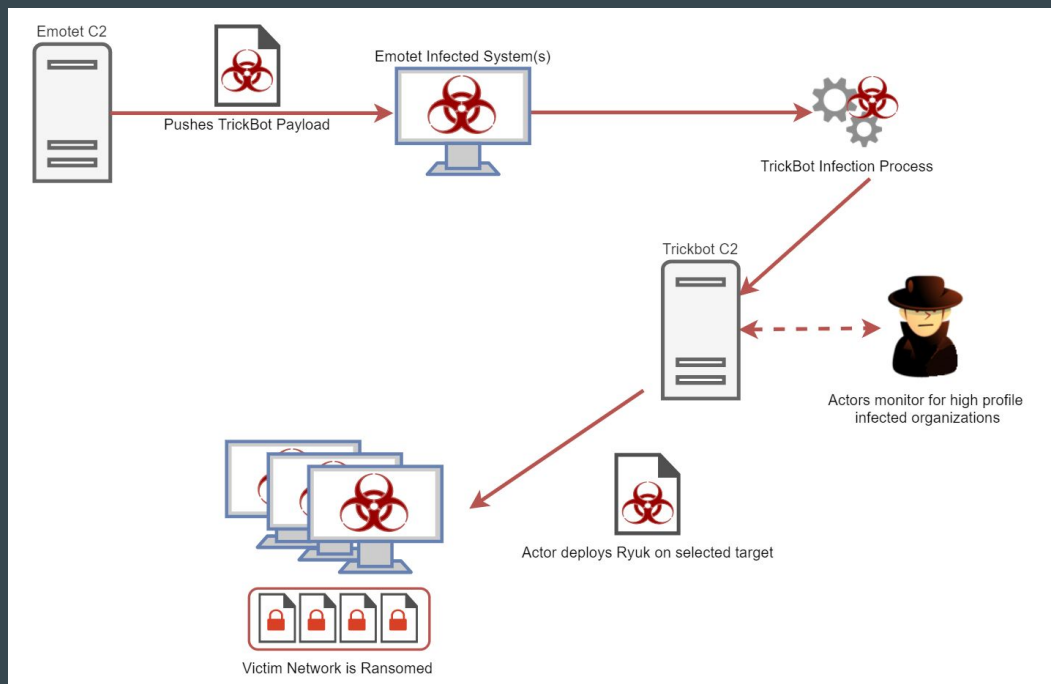
Author: Joie Salvio (Threat Response Engineer)

With online banking becoming routine for most users, it comes as no surprise that we are seeing **more banking malware** enter the threat landscape. In fact, 2013 saw almost a million new banking malware variants—double the volume of the previous year. The rise of banking malware continued into this year, with new malware and even new techniques.

Just weeks after we came across **banking malware** that abuses a Windows security feature, we have also spotted yet another banking malware. What makes this malware, detected as **EMOTET**, highly notable is that it “sniffs” network activity to steal information.

Source: Trend Micro

2018: a very clever downloader



Source: Kryptos Logic

↩ Reply

↩ Reply All ▾

➦ Forward

More ▾

From Maggie Reece <michelle.anderson@epc-event.com> ☆

Subject **Aw: #47071 Invoice Notice**

25/01/2019, 22:59

To i [redacted] ☆

Thank you for your help. Please see the attached.

FILE-47071.doc

Maggie Reece
mreece@aisu.org

Sent: Friday, January 18, 2019 15:59

From: "" [mailto:[redacted]]

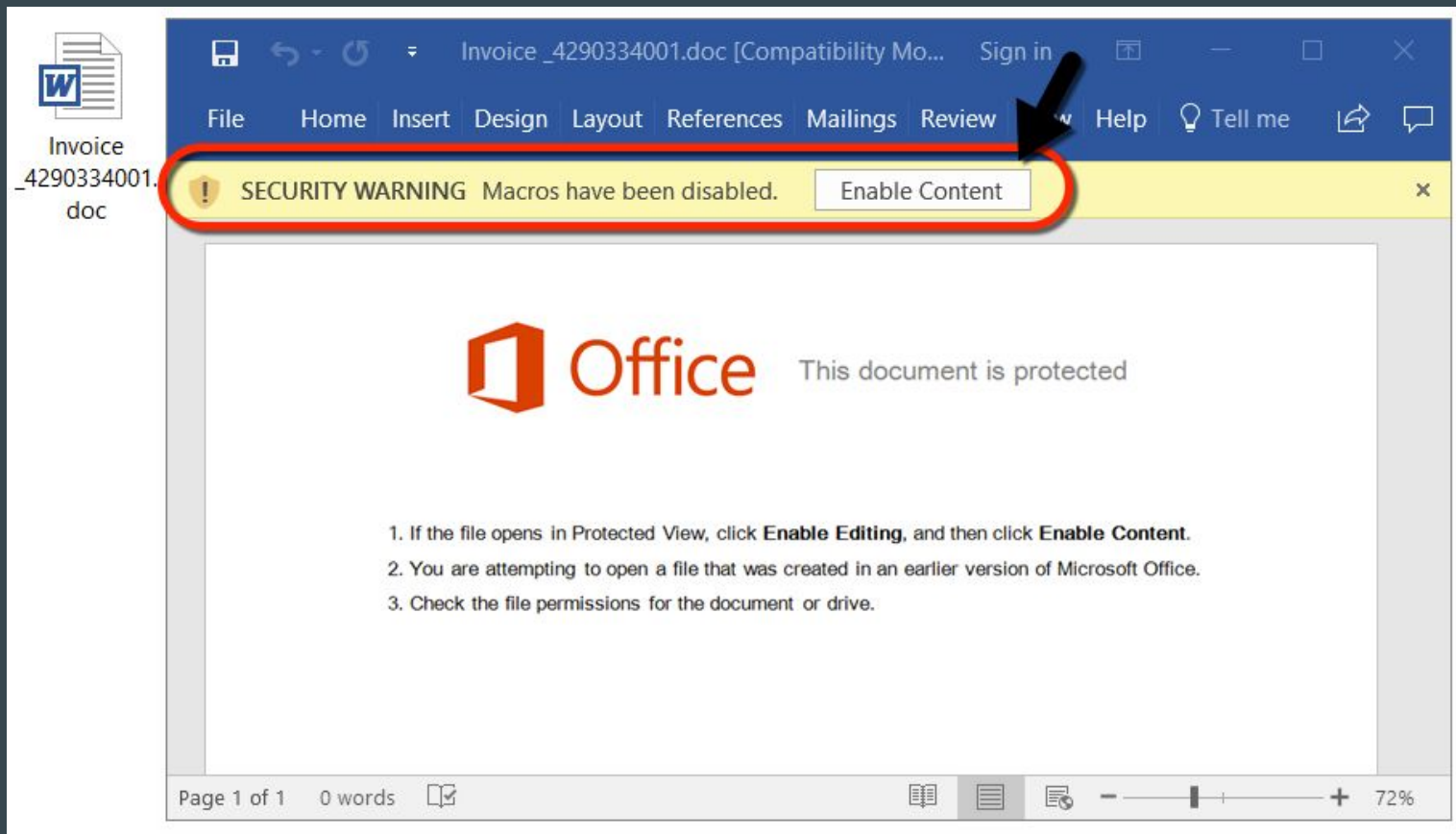
To: "Maggie Reece"

Importance: High

Subject: Aw: Maggie Reece COMET SIGNS PAYMENT NOTIFICATION

▸ 📎 1 attachment: FILE-47071.doc 261 kB

📎 Save ▾



Source: SANS Internet Storm Center

A brief history of macro malware

1990s: macro viruses very prevalent

2000s: Microsoft disables default
execution of macros

2010s: malware authors “kindly ask”
victims to enable macros

Emotet

Lessons learned

Downloaders are what malware attacks pivot around

‘Mass-market malware’ is increasingly prioritizing quantity over quality

Social engineering works

Techniques are barely distinguishable from those used by APT groups

Patchwork

PREVIOUSLY EXAMINED INFORMATION

Let's examine the attribution information we have discussed thus far in this report.

Many of the primary targets of this campaign are regional neighbors of India, and other targets seem to be targeted (by their interests, occupation, and by the content of the spear phishing) to issues affecting India. Circumstantially, this targeting correlates with intelligence requirements necessary for a pro-Indian entity.

However, we felt this was not enough to draw direct conclusions. What we believe makes this correlation much stronger and hints that this is a pro-Indian or Indian entity, is the addition of time of day activity analysis as detailed below.

Source: Cymmetria

APT

Advanced-enough Persistent Threats

Filename	The_Four_Traps_for_China.doc
File Size	4428595 bytes
MD5	7659c41a30976d523bb0fbb8cde49094
SHA1	3f1f3e838a307aff52fbc5bba5e4c8fe68c30e5
Notes	Malicious RTF document that exploits <u>CVE-2017-8570</u> and drops <u>QuasarRAT</u> file qrat.exe.

Source: Volatility

[Security Update Guide](#) > Details

CVE-2017-8570 | Microsoft Office Remote Code Execution Vulnerability

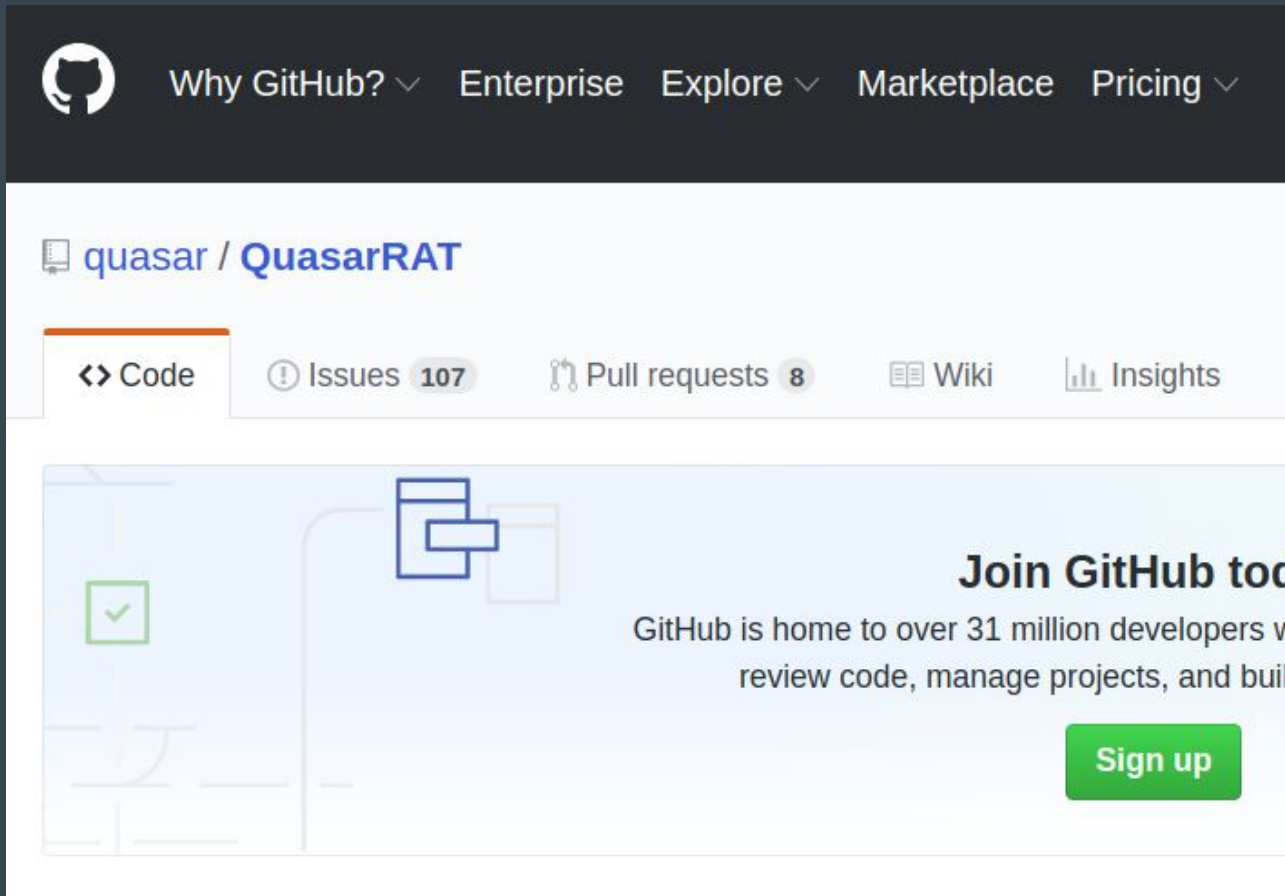
Security Vulnerability

Published: 07/11/2017

[MITRE CVE-2017-8570](#)

A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker could use a specially crafted file to perform actions in the security context of the current user. For example, the file could be used to log on a user with the same permissions as the current user.

Source: Microsoft



The screenshot shows the GitHub interface for the repository 'quasar / QuasarRAT'. At the top is a dark navigation bar with the GitHub logo and links for 'Why GitHub?', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing'. Below this, the repository name 'quasar / QuasarRAT' is displayed. A horizontal menu contains tabs for 'Code', 'Issues' (with 107 issues), 'Pull requests' (with 8 pull requests), 'Wiki', and 'Insights'. The 'Code' tab is selected. Below the menu is a large banner with a light blue background. On the left side of the banner is a diagram showing a green box with a checkmark, a blue box, and a yellow box connected by lines. On the right side of the banner, the text reads 'Join GitHub today' followed by 'GitHub is home to over 31 million developers who review code, manage projects, and build'. A green 'Sign up' button is located at the bottom right of the banner.

Why GitHub? ▾ Enterprise Explore ▾ Marketplace Pricing ▾

quasar / QuasarRAT

<> Code ! Issues 107 🔗 Pull requests 8 📖 Wiki 📊 Insights

Join GitHub today

GitHub is home to over 31 million developers who review code, manage projects, and build

[Sign up](#)

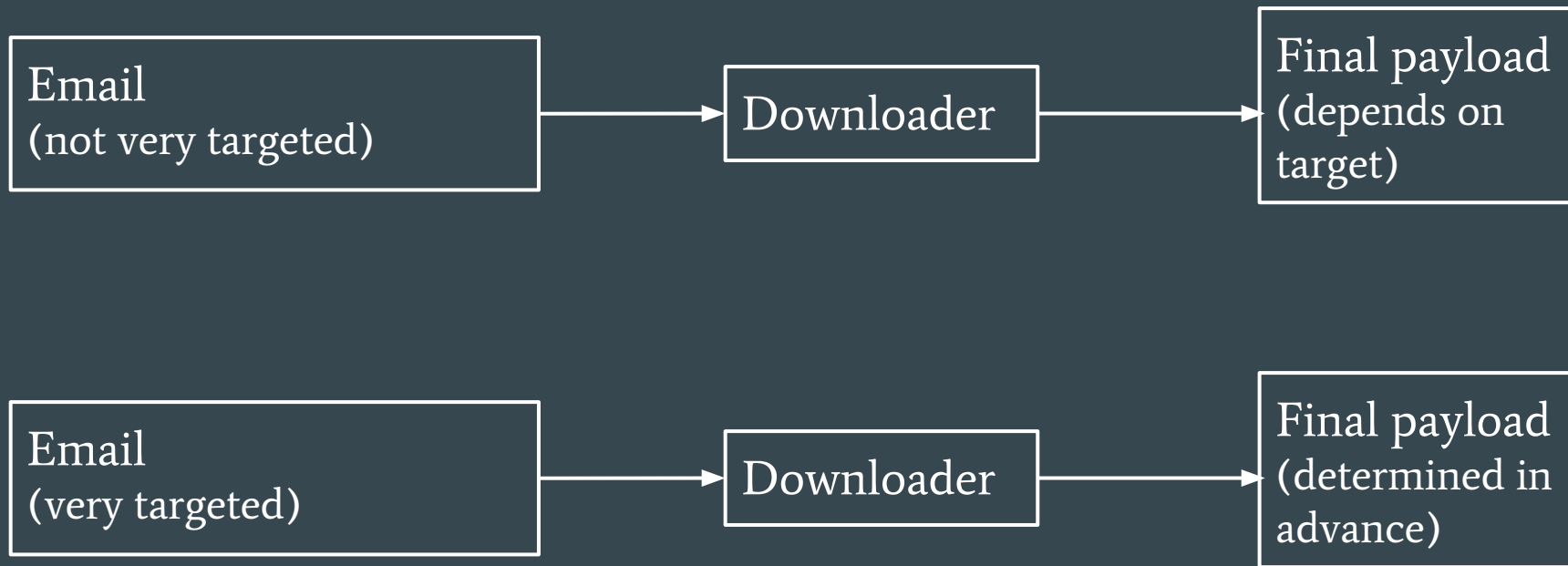
Source: open

BITTER APT group

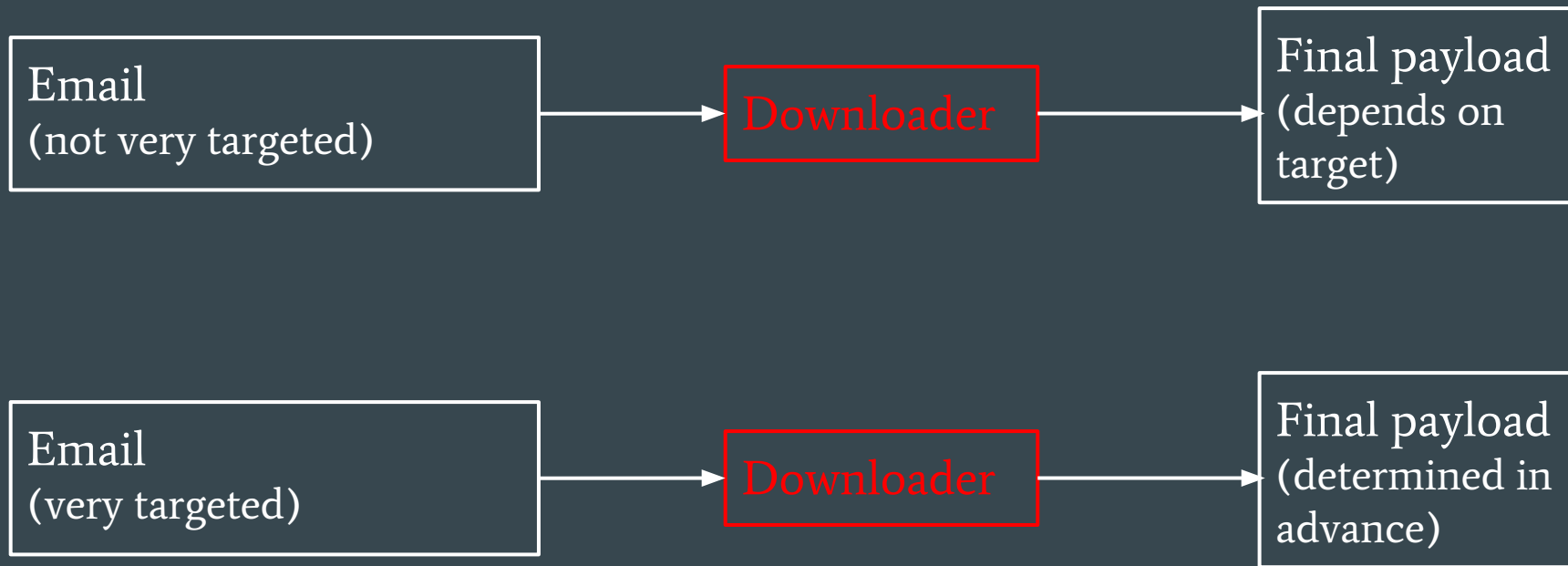
Between November 2018 and January 2019, an engineering and hydraulics company in Pakistan, almasoodgroup[.]com was observed hosting two AtraDownloader executables as well as a malicious document used to deliver a payload. One of the files, Port Details.doc is an RTF document crafted to exploit the EQNEDT vulnerability [CVE-2017-11882](#). This file downloaded a payload that also communicated with the domain hewle.kielsoservice[.]net. The other two files hosted on the engineering company's domain communicated with command and control domain xiovo426[.]net.

Source: Palo Alto Networks

Emotet et al vs Patchwork et al



Emotet et al vs Patchwork et al



Downloaders

give code execution on the machine



Jessica Payne

@jepayneMSFT

Follow



Replying to [@GossiTheDog](#)

If you want a playbook for how to defend your network against infection and lateral movement by a sophisticated attacker, detect and defend against Emotet. The mitigation and investigation techniques line up across multiple adversary sets and have remarkable Return on Investment.

8:39 PM - 2 Jan 2019

Patchwork

Lessons learned

APTs aren't that different from the more advanced commodity malware

Exploit gullible humans and unpatched systems

It's all about the downloader

Pegasus

Operator name	Dates operator was active	Suspected country focus	Political themes?	Suspected infections
CHANG	Jan 2018 – present	Asia	–	Thailand
GANGES	Jun 2017 – present	–	Yes	Bangladesh, Brazil, Hong Kong, India, Pakistan
MERLION	Dec 2016 – present	–	–	Singapore
TULPAR	Feb 2017 – present	Kazakhstan	–	Kazakhstan
SYRDARYA	Sep 2016 – present	Uzbekistan	–	Kazakhstan, Kyrgyzstan, Tajikistan, Turkey, Uzbekistan

Source: The Citizen Lab

Zero-days

The Trident Exploit Chain:

- [CVE-2016-4657](#): Visiting a maliciously crafted website may lead to arbitrary code execution
- [CVE-2016-4655](#): An application may be able to disclose kernel memory
- [CVE-2016-4656](#): An application may be able to execute arbitrary code with kernel privileges

Source: The Citizen Lab

Pegasus

Lessons learned

Zero-days are used in some targeted attacks

Zero-days are often poor ROI

Defending against zero-days is often*
poor ROI

* but not always

Stalkerware

Spyware is getting cheaper, Indian digital beware says EFF

Galperin who was attending India's largest cyber security conference Nullcon 2018 said that mobile phones is the primary attack platform and mobile tracking is one of the fastest growing modes of spying worldwide.

Source: The Economic Times (and Nullcon 2018)

FLEXISPY



24/7 +1 213 810 3122

PRODUCTS

FEATURES

COMPATIBILITY

REVIEWS

SEARCH

MORE

**Many Spouses Cheat.
They All Use Cell Phones.**

Their cell phone will tell you what they won't.



Source: Motherboard

Abusive relationships

They're abusive.
And they're relationships.

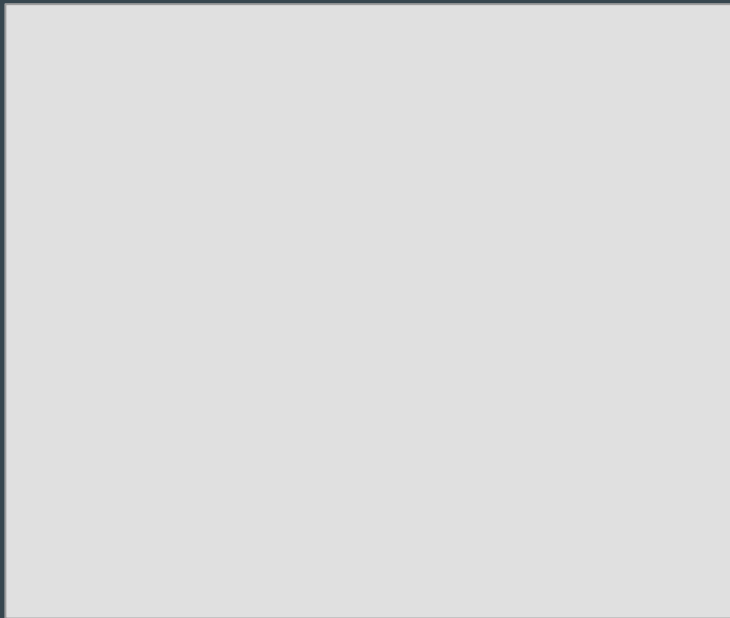
Stalkerware

Lessons learned

Just because something is outside our standard threat model, doesn't mean it can't cause serious damage.

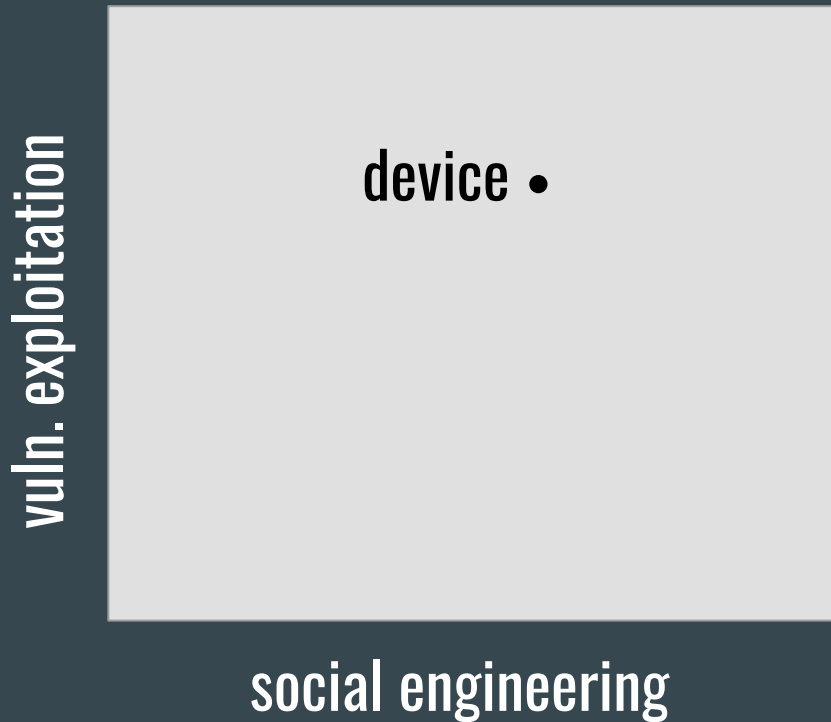
The malwareability chart

vuln. exploitation

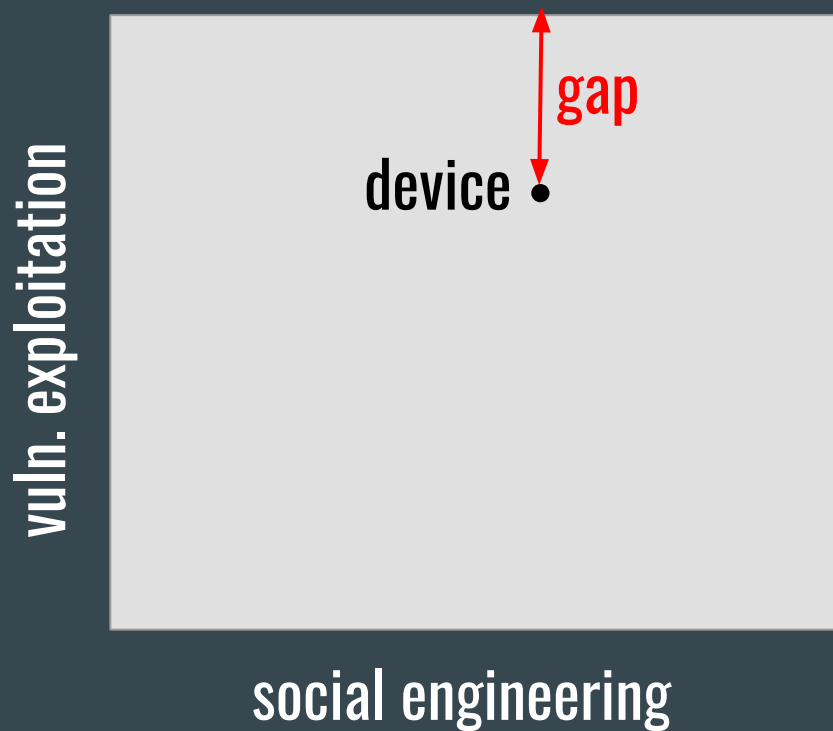


social engineering

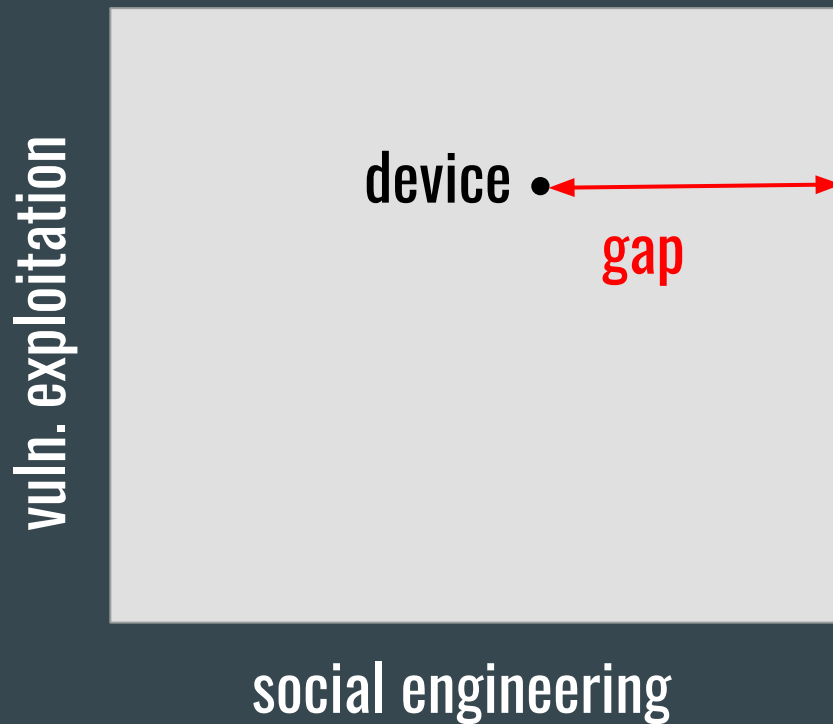
The malwareability chart



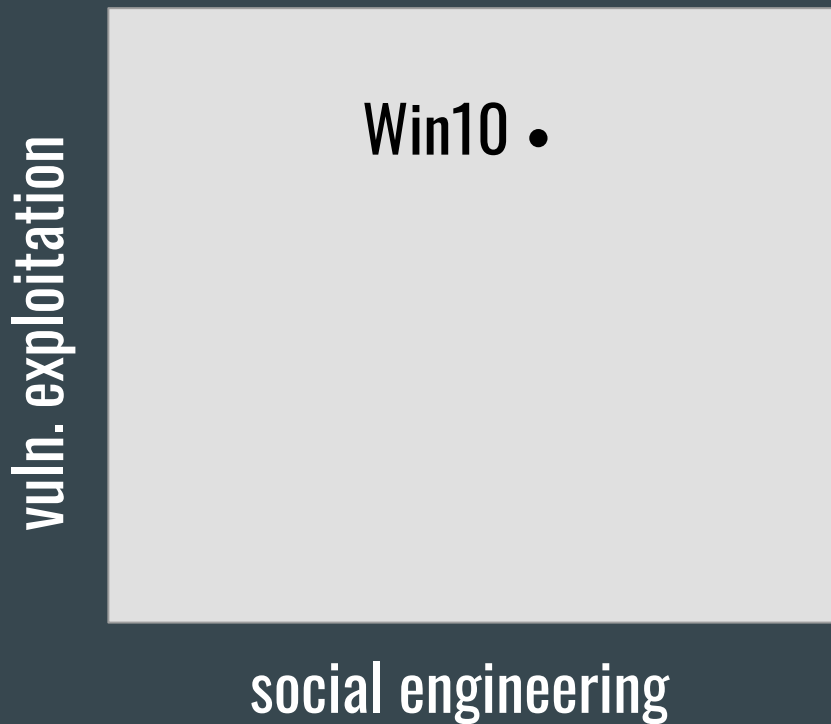
The malwareability chart



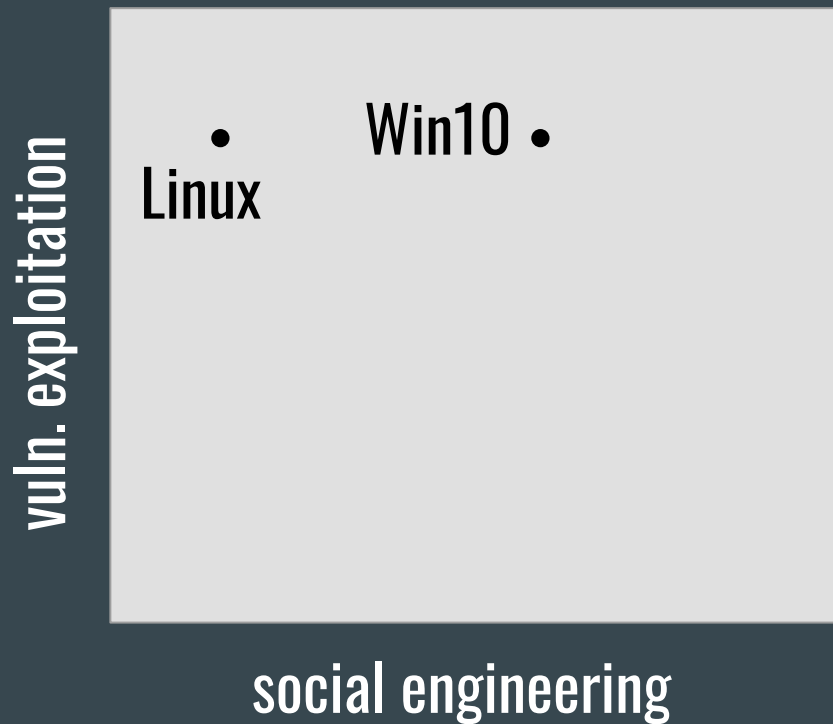
The malwareability chart



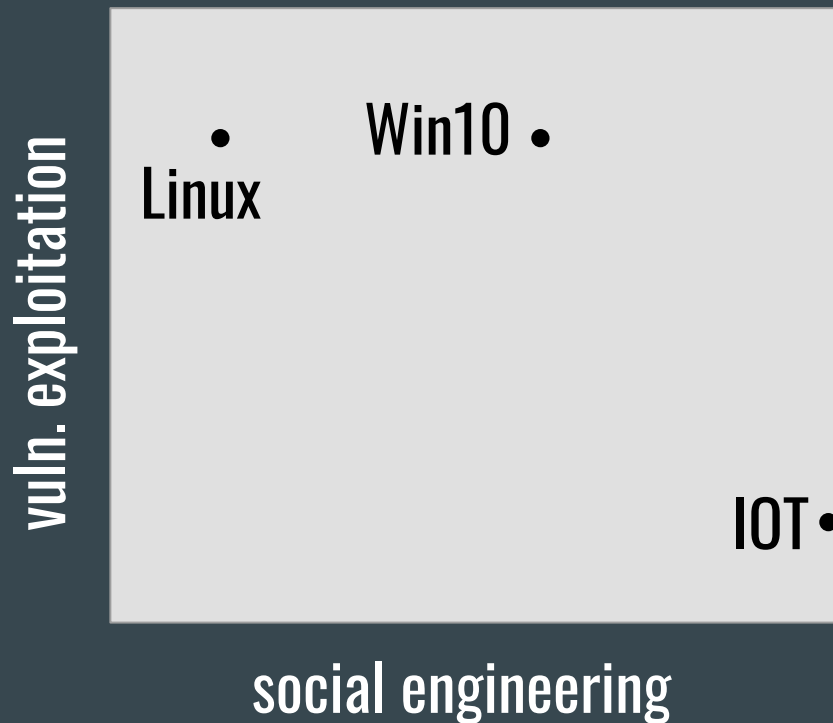
The malwareability chart



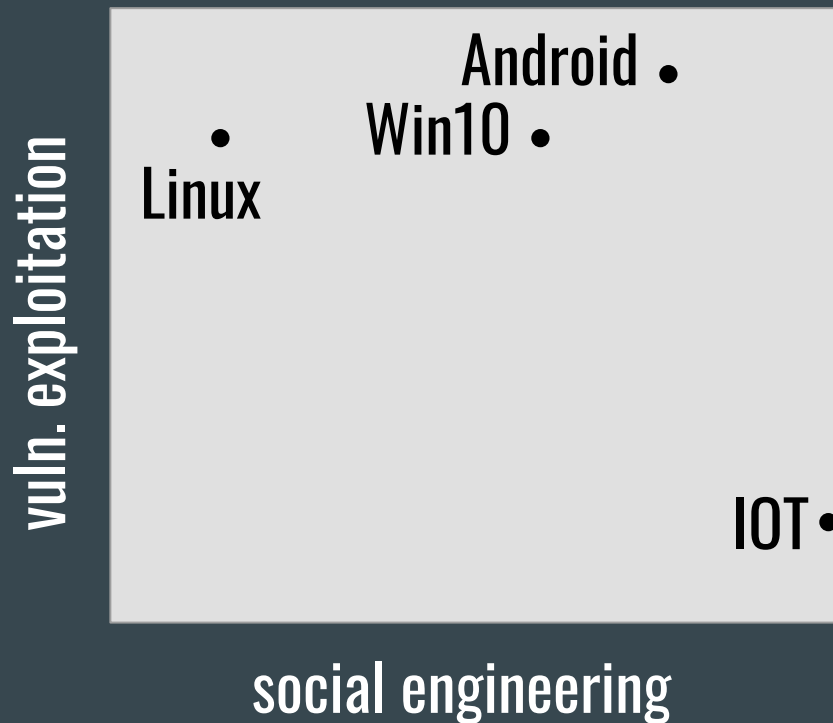
The malwareability chart



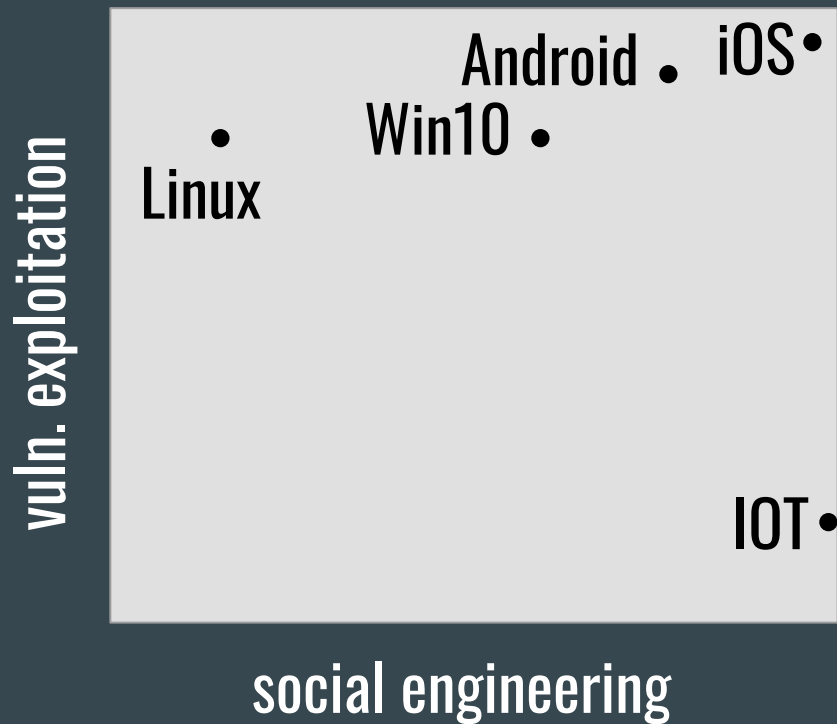
The malwareability chart



The malwareability chart

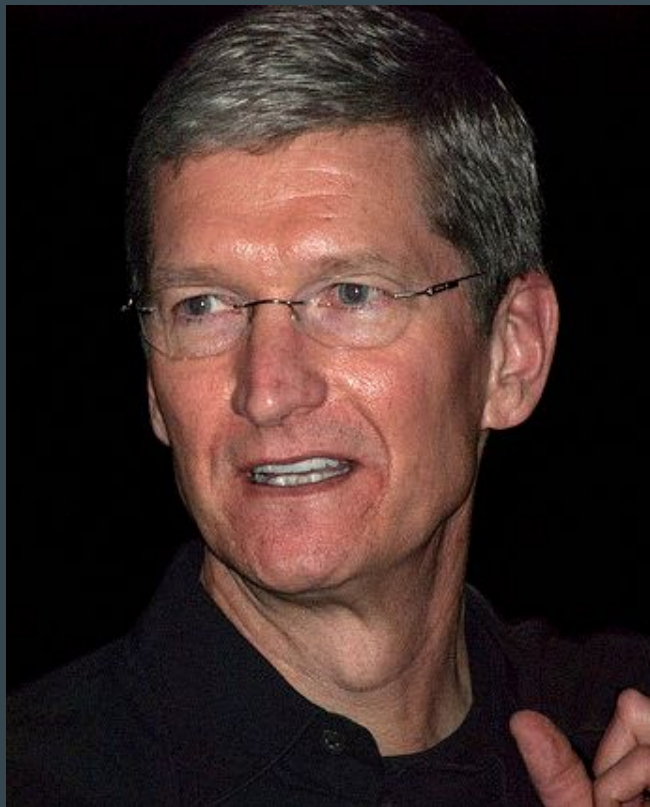


The malwareability chart



The world's best antivirus

The world's best antivirus





@mikko

@mikko

Following



iPhone is 10 years old today. After 10 years, not a single serious malware case. It's not just luck; we need to congratulate Apple on this.

7:53 PM - 28 Jun 2017

10,909 Retweets 15,409 Likes



183



11K



15K



RISKY BUSINESS

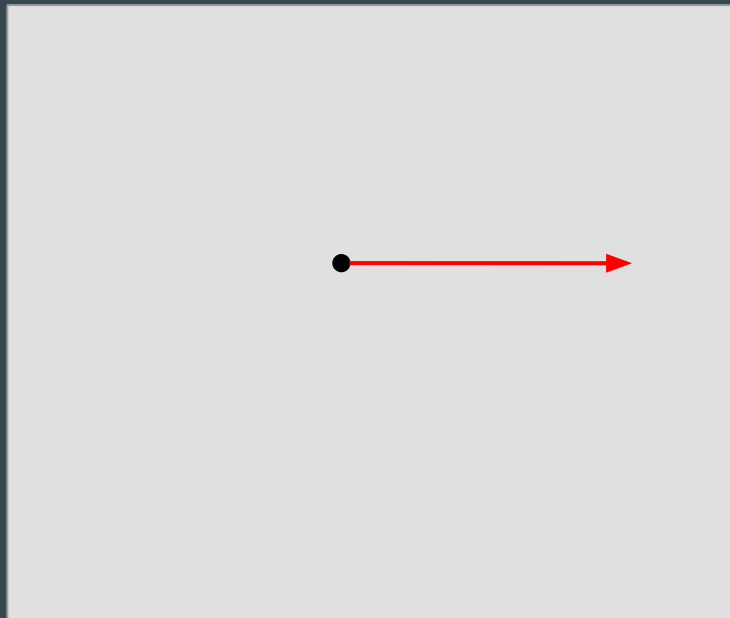
Tim Cook is defending Apple's removal of VPN apps from its Chinese app store with a familiar refrain

By [Josh Horwitz](#) • August 2, 2017

Source: Quartz

Security 'training'

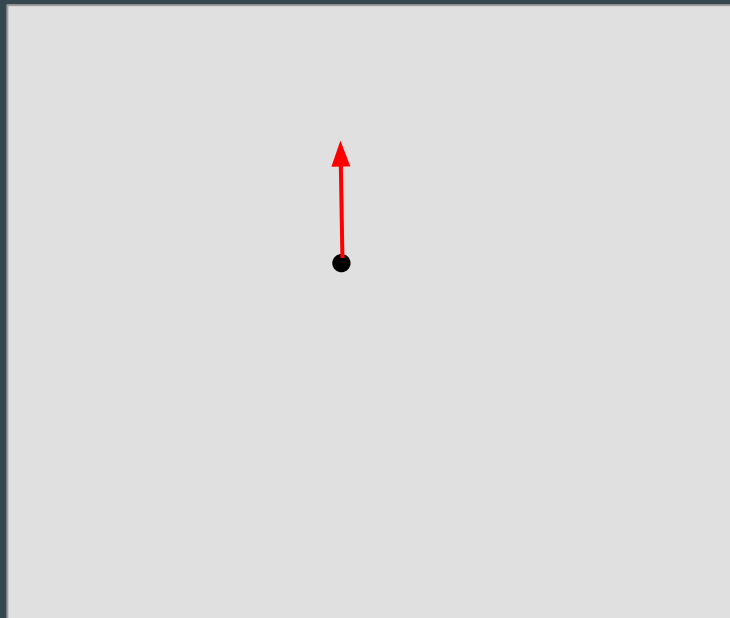
vuln. exploitation



social engineering

Patching

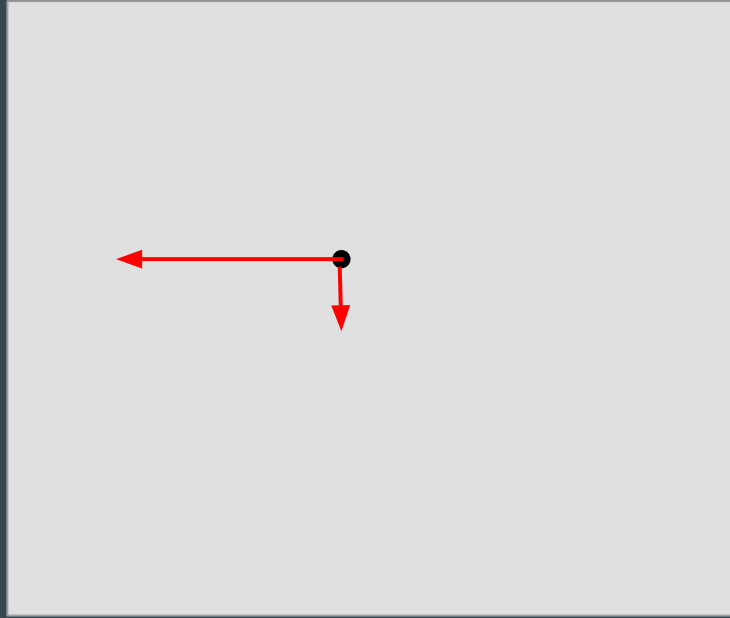
vuln. exploitation



social engineering

Rooting

vuln. exploitation



social engineering

Antivirus

vuln. exploitation

device



social engineering

YMMV

your mileage may vary

A third dimension

‘Scalability’

Conclusion

Lessons learned

Large botnets mostly used for ‘dumb’ things

For more ‘interesting’ attacks, it’s all about the downloader

Zero-days do matter, but only for some

Vulnerabilities and social engineering both matter

The end

Questions?

martijn.grooten@virusbulletin.com

Twitter: [@martijn_grooten](https://twitter.com/martijn_grooten)

LinkedIn: [martijngrooten](https://www.linkedin.com/in/martijngrooten)
