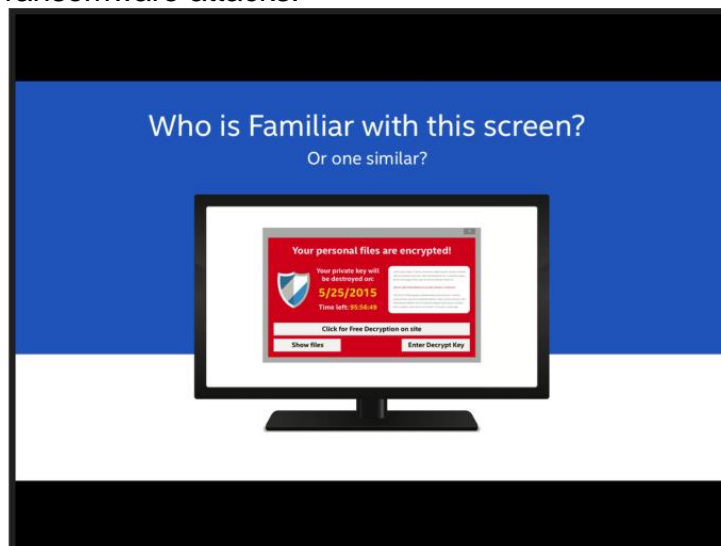


8 Ransomware & How to Defend Against it

Ing. Felix Edlmann, MSc
Helix IT Consulting
edlmann@helix.at

In the following slides you will discover how ransomware attackers deliver their malicious software and which techniques they most commonly employ. You'll find out how you can leverage process, procedure, and advanced technology to reduce the risk of becoming a ransomware victim. Finally, you'll learn how to recover from a successful ransomware attack and how to implement additional protection measures to guard against ransomware attacks.



Ransomware taking over an endpoint, with removal instructions.



Ransomware taking over an endpoint



Digital Transformation of Crime

No criminalization of digital business

But: Digital transformation of criminal business

Simplest proof: CEO / President fraud

December 2015 FAAC € 50.000.000,--

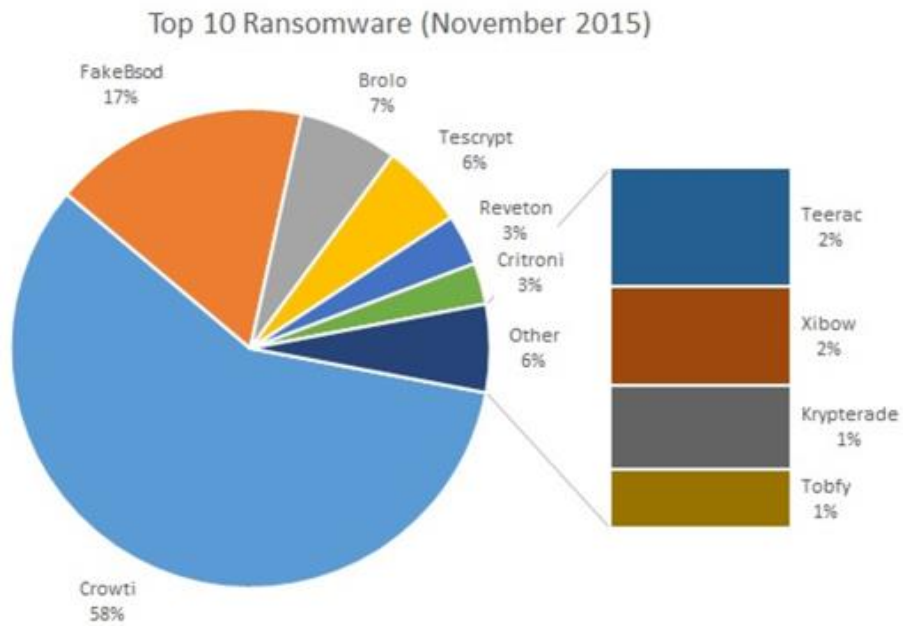
Ransomeware

Type of malware

Typically a Trojan attack

**Access denial type attack, encrypt
all files on your PC**

Goal to get money



Source: Microsoft

How does ransomware work - 5 steps

Targeting

Propagation

Exploit or user activity - 23% open phishing mails, 11% click on attachments; Source: Barracuda

Infection

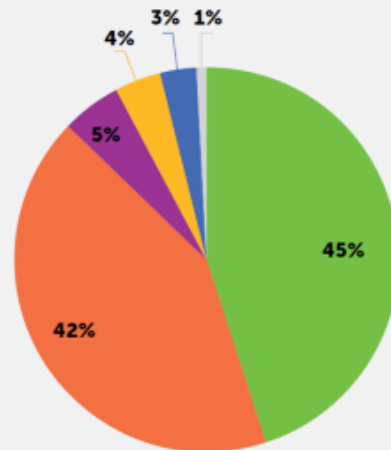
Execution

Layer 8 security Social Engineering Attacks

Vulnerable Applications

VULNERABLE APPLICATIONS USED BY FRAUDSTERS

The graph of vulnerable applications shown opposite is based on information about the exploits blocked by our products. These exploits were used by hackers in Internet attacks and when compromising local applications, including those installed on mobile devices.



The distribution of exploits used by fraudsters, by type of application attacked, 2014

Source: Kaspersky Lab

Advanced Threat

Zero-Day Exploits, Unknown Malware, Advanced Malware

There is no AntiVirus / Intrusion Prevention System Signature

Phishing mail with fake link

22:26 7 of 77 results

Ups

ITwhitepapers Storage A... Tuesday
Battery Technology for Data Centers...
This paper provides a brief overview of
li-ion batteries in comparison to VRLA...

Amazon.de Tuesday
Amazon.de empfiehlt "Brother MFC-8...
Ihr Amazon.de Sonderangebote Felix
Edelmann, MAS, Amazon.de hat neue...

Correlated Magnetics R... Thursday
Correlated Magnetics Research shippi...
[Correlated Magnetics Research Logo]
Hello Felix Edelmann, Your order has b...

derStandard.at Newslet... 04/05/16
Web : Imagetragick: Kritische Lücke ge...
[cid:web.gif]<http://derStandard.at/?
ressort=Web&ref=nl&userid=45117&nl...

trend. Das Wirtschafts... 04/05/16
500-Euro-Schein: Ja oder Nein? | Neu...
Das ist der Header [http://news.trend.at/
templates/fo2de/img/logo.png]<http:...


UPS 04/05/16
Versandbenachrichtigung, Kontrollnum...
[UPS]<http://www.ups.com/content/de/
de/index.jsx?WT.svl=weBmdMk> Diese...

Bookatable 03/05/16
Dein monatlicher Food- und Restauran...
[Dein monatlicher Food- und
Restaurant-Guide]<http://link.ed.book...

Edit

From: UPS >
To: Edelmann Felix >

Versandbenachrichtigung, Kontrollnummer VW26937093
4 May 2016 at 12:13
Inbox



Diese Nachricht wird Ihnen im Auftrag von Koi Discount GmbH zugesandt, um Sie darüber zu informieren, dass die folgenden elektronischen
berfragen wurden. Das/die physische(n)
noch nicht zum Versand an UPS
an tats'achlichen Transportstatus Ihrer
klicken Sie auf den Link zur

<http://depanite.com/ZMX2ei.5AJU/d23rUTayEbxjHDI.php?id=edelmann@helix.at>

Open **ermitteln**

Add to Reading List

Copy

© 2016 United
Marken von U
Hinweise zum
UPS Dienst
Bitte antwort
Bei Fragen und Anregungen kontaktieren Sie UPS kontaktieren.
zeichnen und die Farbe Braun sind eingetragene
shallen.
nicht erhalten.

Diese E-Mail beinhaltet Informationen, die vertraulich oder nicht für die Öffentlichkeit bestimmt sein könnten. Sollten Sie nicht der designierte Empfänger sein, ist das Lesen, Kopieren, Weiterleiten sowie anderweitiger Gebrauch des Inhalts dieser E-Mail unzulässig. Sie werden gebeten, diese E-Mail unverzüglich zu löschen.

22:34 81%

Mailboxes Sent Edit

Edelmann Felix 22:33
WG: Spam ? Ihre Amazon.de Bestellun...
-----Ursprüngliche Nachricht-----
Von: Amazon.de [mailto:admin@amazon.de...]

Edelmann Felix 11:05
Fwd: Kellergassenfest Etsdorf und Bad...
Ing. Felix Edelmann, MAS Helix IT
Consulting e.U. Wienerstrasse 18-20/5...

schnell@prd.at 08:08
Einladung: FWF Am Puls: Soziale Netz...
Sehr geehrte Frau Schnell! Bitte melden
Sie mich zu dieser Veranstaltung an....

Guenduez Ugur Yesterday
AW: Kontaktdaten
Mit freundlichen Grüßen Ing. Felix
Edelmann, MAS Helix IT Consulting e...

Casanova Alexander Tuesday
AW: comDIALOG mit Multitmatk
Sehr geehrter Herr Casanova! Danke für
Ihr Angebot für die multiMATIC 700 ml...

Federspiel Eveline Tuesday
AW: Termin
Liebe Eveline! Danke für die Einladung
wir kommen zu dritt. Liebe Grüße Felix...

Schiehl Tuesday
AW: 2 Sitzung
Liebe Familie Schiehl! Wie am 03. Mai
2015 besprochen sende ich Euch unse...


Updated Just Now

To: Edelmann Felix >
From: Edelmann Felix >

WG: Spam ? Ihre Amazon.de Bestellung: #366-2137259 von "Samsung Photo-VW99994..." und 1 andere(r) Artikel
Today at 22:33

-----Ursprüngliche Nachricht-----
Von: Amazon.de [mailto:admin@amazon.de]
Gesendet: Montag, 21. März 2016 13:06
Betreff: Spam ? Ihre Amazon.de Bestellung: #366-2137259 von "Samsung Photo-VW99994..." und 1 andere(r) Artikel

Wir freuen uns auf Ihren nächsten Besuch!



Amazon-Qulttung.
21.03.16.5237

Advanced Threat Defense ATD

Local:

Sandbox

www.sandboxie.com

Cloud based:

Exchange Online Advanced Threat Protection

www.microsoft.com

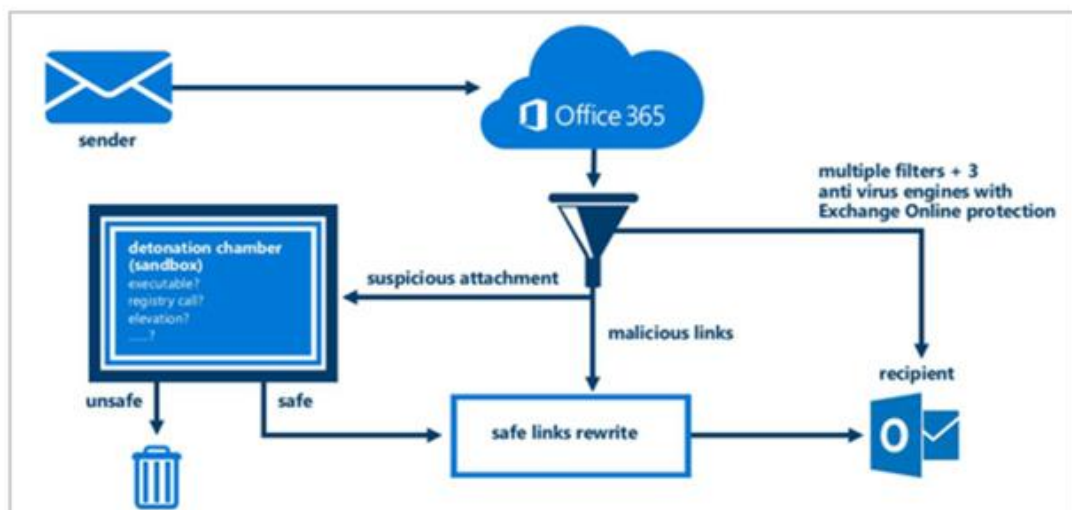
Barracuda Essentials for Office 365

www.barracuda.com

McAfee ATD, Intel Security, Cisco Cyber Threat Defense,

...

Exchange Online Advanced Threat Protection

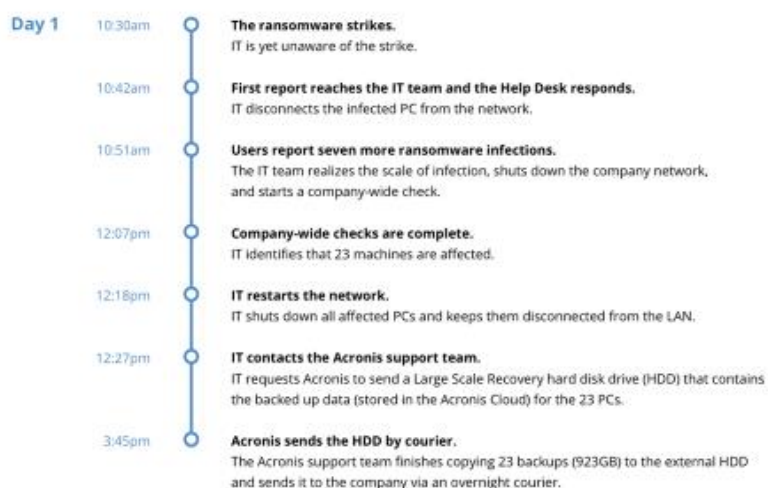


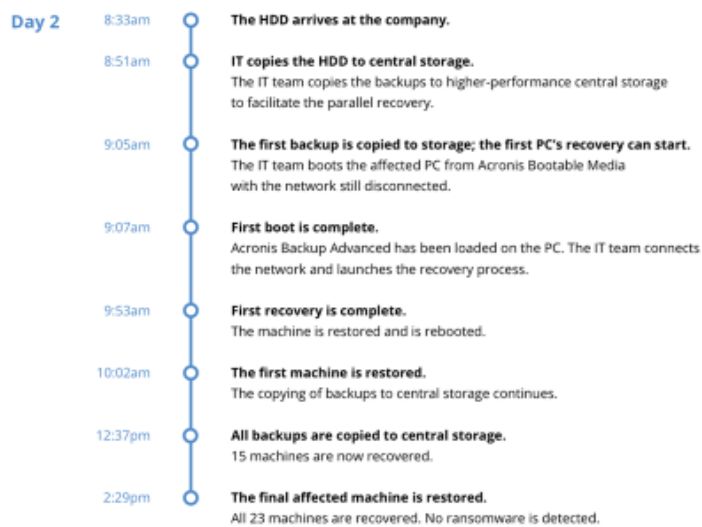
What to do if:

- Alert law officials
- Isolate the affected machine
- Remediate actions
- Restore from back-up
- Pay the ransom ???

Ransomware Strikes

The ransomware affects numerous machines in the company, and the company IT team invokes the recovery plan. Here is the timeline.





Prevent Infection

- Apply all Updates and Security Patches immediately
- Have a "recent" back-up, online with automatic sync
- Remove the administrator right from yourself
- Don't open phishing mails
- Don't click on attachments
- Don't click suspected links
- Use Advanced Threat Defense

Your best defense: Back up, Back up, Back up...