IS MALWARE THE NEW WEAPON OF MASS DESTRUCTION?

Tony Anscombe
Global Security Evangelist
ESET
tony.anscombe@eset.com
@tonyatESET
Title 18 U.S.C. §2332a defines weapons of mass destruction (WMD) as:

- Any explosive, incendiary, or poison gas, including the following: a bomb; grenade; rocket having an explosive or incendiary charge of more than four ounces; missile having an explosive or incendiary charge of more than one-quarter ounce; mine; or device similar to any of the previously described devices;

- Any weapons that is designed or intend to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;

- Any weapon involving a disease organism; and

- Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.
Malware of Mass Disruption

- Malware of Mass Disruption (MMD) as:
- Any exploit, virus, worm, Trojan horse, ransomware, spyware, adware or scareware and any other intentionally harmful computer program;
- Any software that is intended to damage or disable computers and computer systems;
- Any phishing attempt to obtain sensitive information such as usernames, passwords, credit card details for malicious reasons;
- Any data breach of sensitive, protected or confidential data
EVOLUTION OF MALWARE

1980s
Malware destroys data and corrupts systems

Elk Cloner
Infected Apple’s OS

1982
Rick Astley
Never Gonna Give You Up

1987
50% US homes online
Antivirus industry grows

1982
Social e
Law en
The Malware Trend
New Malware Trend
The Havex

- June 2014
- Remote access trojan
- Attacked industrial systems
- European companies
- Industrial applications
- Analysis for future attacks
Black Energy

- 2015
- Trojan to conduct DDoS attacks
- Attacked SCADA/ICS companies
- Energy markets globally
- ICS/Energy/Government - Ukraine
- Spear phishing
- December 2015 – 6 hour darkness
Industroyer

- December 17 2016 Ukrainian power outage
- 75 minute blackout
- Industrial Control System
- Well funded, dedicated, persistent attacker
- 2nd Attack on Ukraine power systems—Black Energy 2015
Top Democrat's emails hacked by Russia after aide made typo, investigation finds
Democracy

DHS officials: 21 states potentially targeted by Russia hackers pre-election
U.S. Tells 21 States That Hackers Targeted Their Voting Systems
MEANWHILE...

Phishing email

Malicious attachment

Word

1. EPS (CVE-2017-0261)

Seduploader dropper
(CVE-2017-0263)

Drops

Seduploader payload

WINWORD.EXE

Sedreco/Xagent
WannaCryptor

- Unleashed on May 12
- Similarities link it to Lazarus group
- No geo targeting
- Maybe Chinese origin
- North Korea
- Evidence?
As it happened
The fall out

Hospitals turn patients away as NHS caught up in global ransomware attack

Cyber attack hits German train stations as hackers target Deutsche Bahn

The Telegraph
Not Petya – Bad Rabbit

- Probably Leaked NSA Tool
- Eternal Romance
- Drive by download
- Ransomware
- Ukraine infrastructure
- Kiev Metro
FinFisher

- FinFisher – also known as FinSpy
- Infamous spyware
- FinSpy sold to governments
- Indications of ISP involvement
- Live surveillance capabilities
- ISP-Level MitM attack
FinFisher

ISP LEVEL?

TARGET

www.legitimatewebsite.com

DOWNLOAD LINK

legitimate app

legitimate app trojanized with FinFisher

eset

ENJOY SAFER TECHNOLOGY™

RSA Conference 2018
Gazer

- Espionage campaign
- Attacking diplomats since 2016
- Spear-phishing attack
- South East Europe and former Soviet Union
- Multiple stage backdoor
- Avoids detection
- Possibly - Turla group
Meltdown & Spectre
Cambridge Analytica

Execs from firm at heart of Facebook data breach say they used ‘unattributable and untrackable’ ads, according to undercover expose

‘Utterly horrifying’ Ex-Facebook insider says covert data harvesting was routine

Zuckerberg Social media head summoned by MPs in London

Facebook Is it time we all deleted our accounts?
Conclusion

- Malware of Mass Disruption (MMD) as:
- Any exploit, virus, worm, Trojan horse, ransomware, spyware, adware or scareware and any other intentionally harmful computer program;
- Any software that is intended to damage or disable computers and computer systems;
- Any phishing attempt to obtain sensitive information such as usernames, passwords, credit card details for malicious reasons;
- Any data breach of sensitive, protected or confidential data
Questions