2013+ Global Volume
2017+ Global Volume

- Malicious URL Messages
- Malicious Attachments
2018+ Global Volume
Attack Structures
Threat Details
Abused Attachment File Types

• Most Common
  - Microsoft Office Documents with Macros
  - Microsoft Office Documents with Embedded Object
  - PDF with links

• New
  - XL4 Macro
  - Template Injection

• Other
  - DDE
  - Password protected Microsoft Office Documents
  - Documents that exploit Microsoft Office vulnerabilities
    • Most common is CVE-2017-11882
    • All time highest volume is CVE-2017-0199
Password Protected Documents

• Office documents where passwords are required to open the document
• Password is presented to the user in the body of the email
• Advantages
  – Appears to the user as privileged information contained within the document
  – Evades automated sandbox analysis
• Campaigns tend to use the same password for all samples
• Most recently seen in these campaigns
  – IcedID - TA516 [SmokigDro]
Stella
To: wes@unknown.com
Reply-To: Stella
wes

How are you wes,

You will be charged $3,628.74 on your current Visa balance straightaway. See attachment to avoid it. Password is 1115

Yours truly,

Stef
wes_scan.doc

someone - Message (HTML)

Hello,

Your Visa card ending in XXXX will be charged $3,187.26 shortly. Take a look at attachment for details. Password is 1115.

Thank you.
Delivery Methods - URL

• Most Common
  - Links to phishing pages
  - Direct links to malicious docs / exes
    • Typical case: get the victim to download and open a malicious document/executable from the internet (social engineering)
  - Links to zipped downloader scripts (e.g., zipped .js & 7-Zipped .vbs)

• Newer
  - TDS Style
    • BlackTDS
    • SocGholish
    • SocGoth

• Less common:
  - Links to pages infected by Exploit Kits
You are using an older version of Firefox

Update now to keep your Firefox browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Update Firefox
Malware at the end of links

https://dl.dropbox.com/s/3tsrd9j86idxkzx/Doc.zip?dl=0

0 Messages • 13 Proofpoint Customers • 0 People Impacted

Attack Spread

Targeted: 1 2 3-5 6-9 10+ 20+ 30+ 40+ 80+ 100+ 160+

Widespread: Seen by 13 Proofpoint Customers

Attack Progression

Messages: 0 Blocked 0 Delivered

Delivered Messages: 0 With Rewritten URLs 0 With Non-rewritten URLs

Clicks on Rewritten URLs: 0 Blocked 0 Permitted

Forensics

Reports: Report #1: 2017/05/02 - 15:32 (UTC +00:00) || Windows X.
Unique Malicious URLs
Exploits

• We consider social engineering as an "exploit"
  - Office Macros are an extension of umbrella “Social Engineering” term

• Almost all exploits we see are Microsoft Office exploits
  - CVE-2017-11882
    • By far the most popular
  - CVE-2017-0199
  - CVE-2017-8570

• Exploit Builder Kits
  - ThreadKit
    • Supports multiple CVE’s.
    • Has been found to be using exploit code from researchers
  - LCG Kit
    • Uses different variations of CVE-2017-11882
Global Campaign Exploits (Messages)

- Office VBA Macro
- PowerShell
- Social Engineering
- PDF
- JavaScript
- WMAI
- Thread Hijacking
- Geofencing
- Steganography
- Password-Protected
- CVE-2017-11882
- LCG Kit
- Compressed Executable
- XL4 Macro
- VBS
Malware

• Stealers and Downloaders
  – Dominated 2018
  – 2019 not looking any different

• Top malware 2018
  – Emotet
  – Pony
  – Tordal

• Top Malware 2019
  – Emotet
  – Ursnif
  – IcedID
Actors*

*Not the actors pictured in this slide
TA Designations

- 000 - 499: APT
- 500 - 1999: Crime large
  - large campaigns like those distributing Locky / Dridex bankers and ransomware
- 2000 - 2999: Crime small
  - more targeted like certain small BEC groups
- 3000 - 3999: Crime sophisticated
  - Cobalt, Fin7
- 4000 - 4999: Unknown/Sophisticated/Specialists
  - interesting groups that we are not sure where else to put
TA505

• TA505 tends to lead trends
  - 2014 – Banking Trojan
  - 2015 – Banking Trojan
  - 2016 – Ransomware
  - 2017 – Ransomware
  - 2018 – RATs
  - 2019 – Backdoors/RATs
People Centric Security Analytics (PCSA)
The Defender’s POV

DMZ

Web Servers

Internal vLANs

App and Email Servers

File Shares

Databases

PCs / Printers

O365?
The Attacker’s POV

Jack Barker • 3rd
Executive at Bank Co
500+ connections

Laurie Bream • 2nd
Financial Advisory at Bank Co
500+ connections

Richard Hendricks • 3rd
Senior Systems Administrator
55 connections
Featured Skills & Endorsements
Microsoft Exchange • 49
People-Centric Security Analytics

Leverage our *unique* data to identify individuals or groups within an organization that might present a previously unknown security risk.
Proofpoint Attack Index

Actor Sophistication

Attack Targeting

Type of Attack

Volume of Attacks

• 0-1000 score per threat sent
• Weighted composite score
• Score explanations

Understand the risk your users face and prioritize the most effective compensating controls

Receive reporting and metrics on the threats your users face
Attack Index Results

Recipent Threat Category Breakdown

EA to the CTO
Head of HR
Assistant to Head of Aerodynamics
Head of Hospitality