iT-CUBE SYSTEMS
Member of SecureLink

Abschlussbericht
PROOFPOINT THREAT DISCOVER

AUSWERTUNG:

- Die Anzahl infizierter Mailboxen
- Die Anzahl schadhafter Nachrichten
- Die Anzahl schadhafter URLs
- Die Anzahl schadhafter Attachments
- Welche User und welche Abteilungen am stärksten betroffen sind
- Die Forensische Information zu den Top Malware-Kampagnen

iT-CUBE SYSTEMS AG
Paul-Gerhardt-Allee 24
81245 München, Germany
T: +49 89 2000 148 00
F: +49 89 2000 148 29
info@it-cube.de
www.it-cube.de

THREAT SUMMARY

1174	1,447,907	21	15	AD Server
Mailboxes reviewed	Messages scanned	Active Campaigns	Malware Families	Dtadldap.dealer-tire.com

	Infected Mailboxes	Malicious Attachments	Malicious Messages	Malicious URLs
Known Threats	38	32	90	17
Potential Threats	343	3375	32	30.618

Im Anschluss an unseren ausführlichen Report beraten wir Sie gerne über die weiteren nächsten Schritte, was getan werden kann, um Ihre Umgebung noch sicherer zu machen und besser gegen Angriffe von außen zu schützen.

CAMPAIGNS, MALWARE & TOP DEPARTMENTS

Campaigns seen: 21

- Personalized Nymaim – 6th April
- Dridex Botnet 301 – 13th April
- Personalized Nymaim – 5th April
- Vawtrak 80 – 5th April
- Websites Infected with Angler Exploit Kit – March
- Dropbox Account Phishing –May
- Personalized Nymaim – 13th April
- Vawtrak 80 – 6th April
- Dridex Botnet 122 – 13th April
- Vawtrak 80 – 31st March
- Cerber – 28th April
- Google Drive Phishing – April
- Websites Infected with Angler Exploit Kit – April
- Personalized Nymaim – 25th April
- Cerber – 3rd May
- Google Drive Phishing – March
- Adobe Account Phishing – April
- Dridex Botnet 220 – 18th March
- Personalized Nymaim – 26th April

Malware detected: 15

- Nymaim
- Andromeda
- Send-safe Enterprise Mailer
- Alphacrypt
- Ursnif
- Cerber
- Dridex
- Tinba
- Smoke Loader
- GootKit
- CryptoWall
- Locky
- Pony
- Vawtrak
- Bedep (TBD)

Departments affected

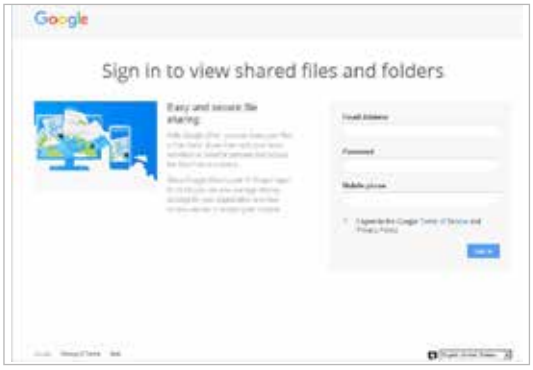
- Outside Sales
- Human Resources
- Marketing
- IT infrastructure
- Warehouse
- Program Management
- Inside Sales
- Sales – Tire Store
- Information Solutions
- Logistics

CREDENTIAL PHISH: Google Drive Phishing

Attackers attempt to steal a victim's Google account credentials through the use of a fake Google Drive login page.

Proofpoint global:
At least 1.489 Proofpoint customers affected

Impact: Credential Theft



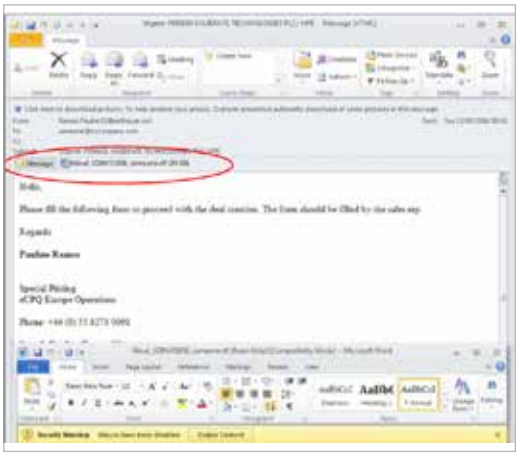
ATTACHMENT CAMPAIGN: Dridex

Messages from random senders containing a MS Word macro-enabled attachment.

Proofpoint global:
4.529.777 Messages // 1.327 Customers targeted

Impact: Dridex

- Attackers harvesting banking credentials and other personally identifiable information.
- Credit information, SSN and banking info highly desirable



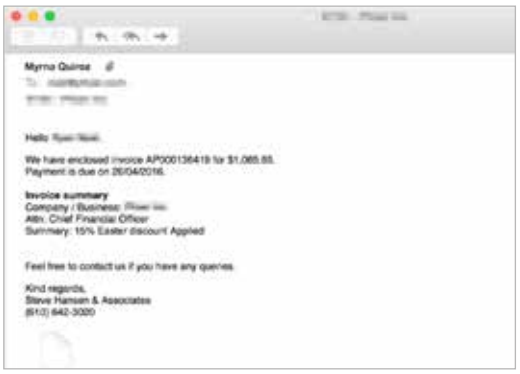
MALWARE CAMPAIGN: Nymaim

- Targets finance
- Message: Urgent missed payment /w MS Word document

Proofpoint global:
1.000+ Proofpoint customers

Impact: Nymaim

- Banking Trojans & Ransomware
- Recent attacks spread using established E-Mail marketing services to avoid blacklists and detection tools.
- Loads additional payloads of Pony and Ursnif (ransomware)



MALWARE CAMPAIGN: Websites infected with Angler Exploit Kit

Infected websites exploit vulnerable web browsers with the Angler Exploit Kit.

Proofpoint global:
Over 1.200 customers affected

Impact: Angler

- Ransomware delivery vehicle (almost any payload can be delivered)
- Angler EK multiple malware options
  - Ransomware, keyloggers, wire-fraud
  - Recently: Alphacrypt / Teslacrypt

MALWARE CAMPAIGN: Vawtrak

Banking Trojan spreads via attachment-based phishing E-Mail, leverages social media and exploits kits Angler EK

Proofpoint global:
At least 920 Proofpoit customers affected

Impact: Vawtrak

- Banking credential theft – Command & Control Server
- Keylogging & desktop screenshots
- Logging visited websites, digital certificate theft
- Granting remote access