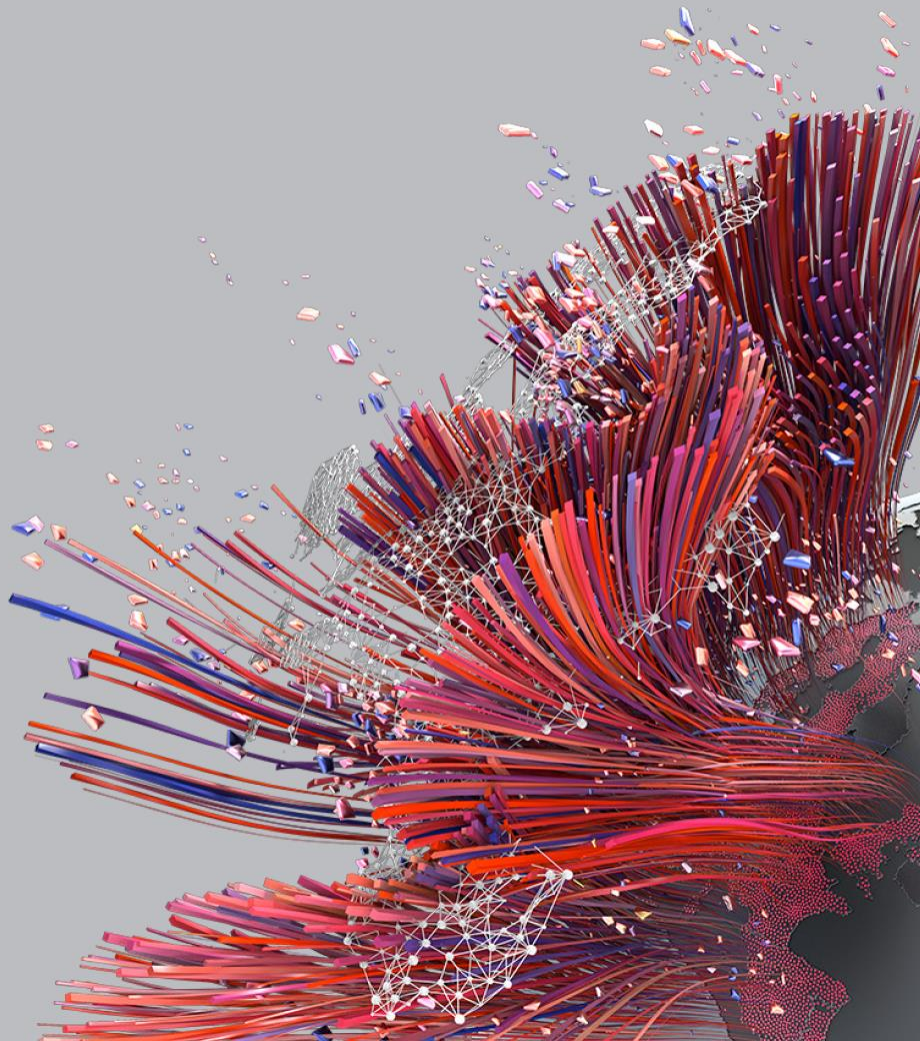
Incident Response engaged, what now?

Lucas van den Berg
Sr. Incident Response Coordinator



Serhiy Lunak
Analyst

Rense Buijen
Director

David Walsh
Analyst

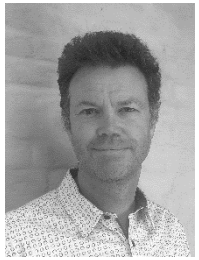
Matthias Schönhofer
Coordinator

Marc Lanzendorfer
Analyst

incident_response@trendmicro.com

Lucas van den Berg
Coordinator

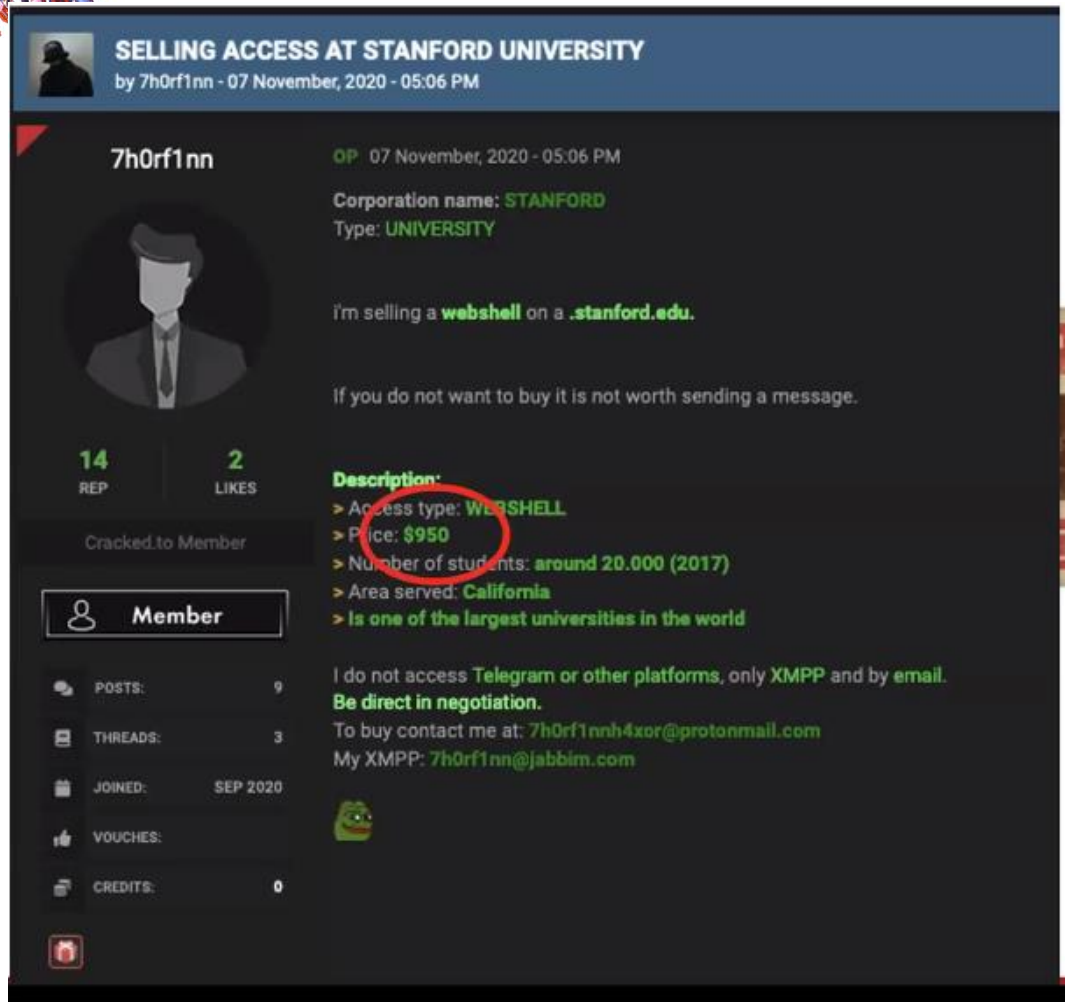
Cenen Enalbes
Analyst



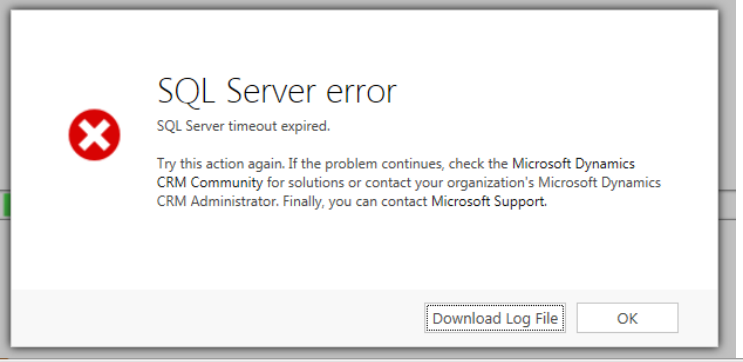
Raf Hoogstijns

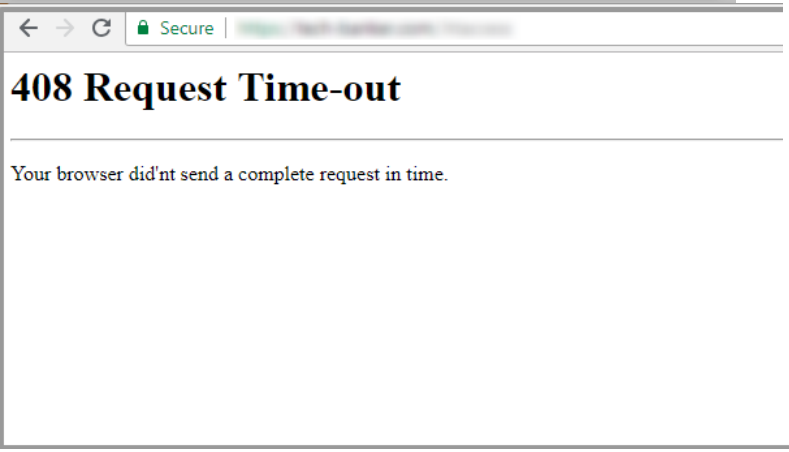
Mikkel Madsen
Analyst

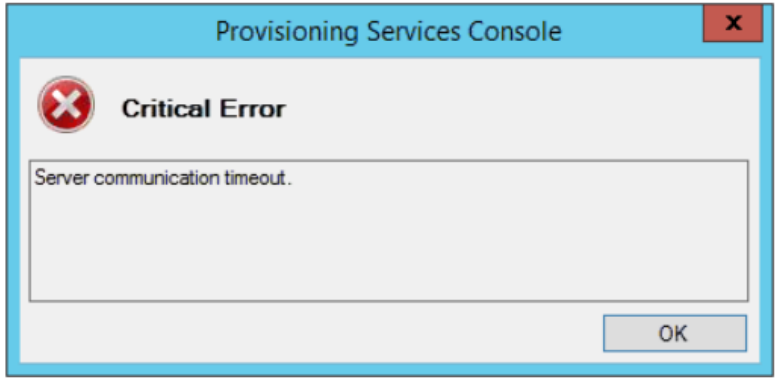
© 2021 Trend Micro Inc.



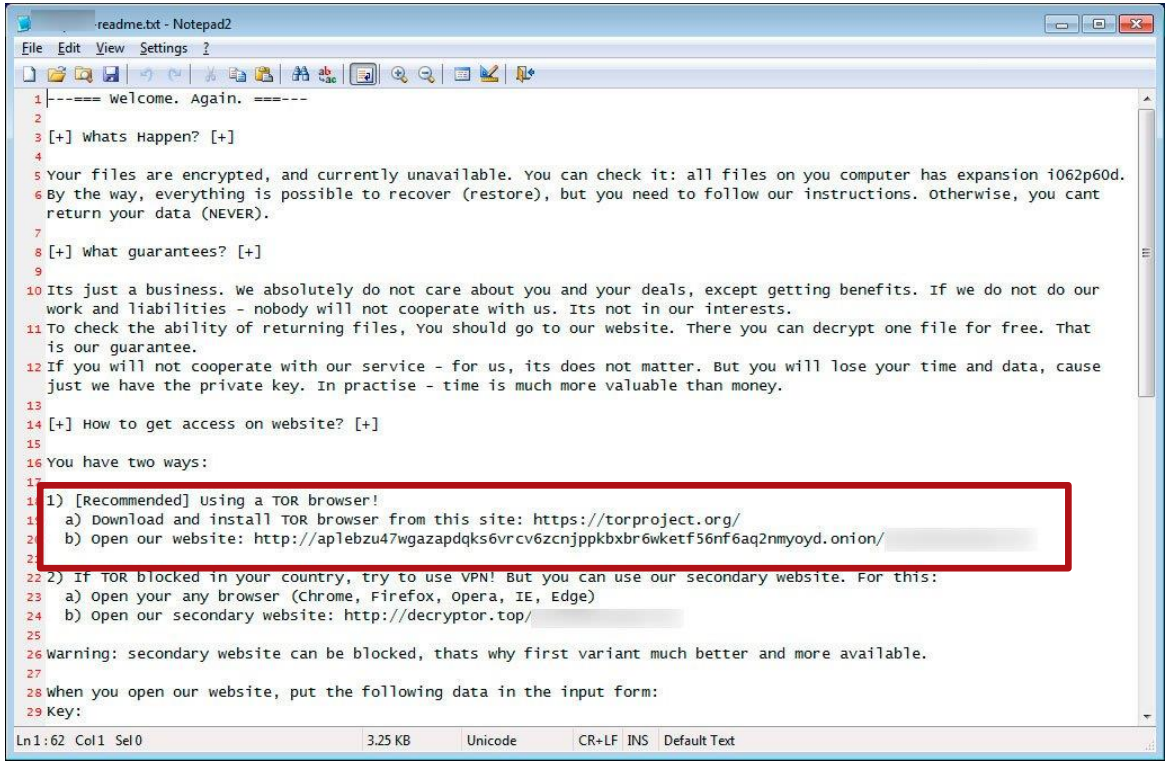
© 2021 Trend Micro Inc.



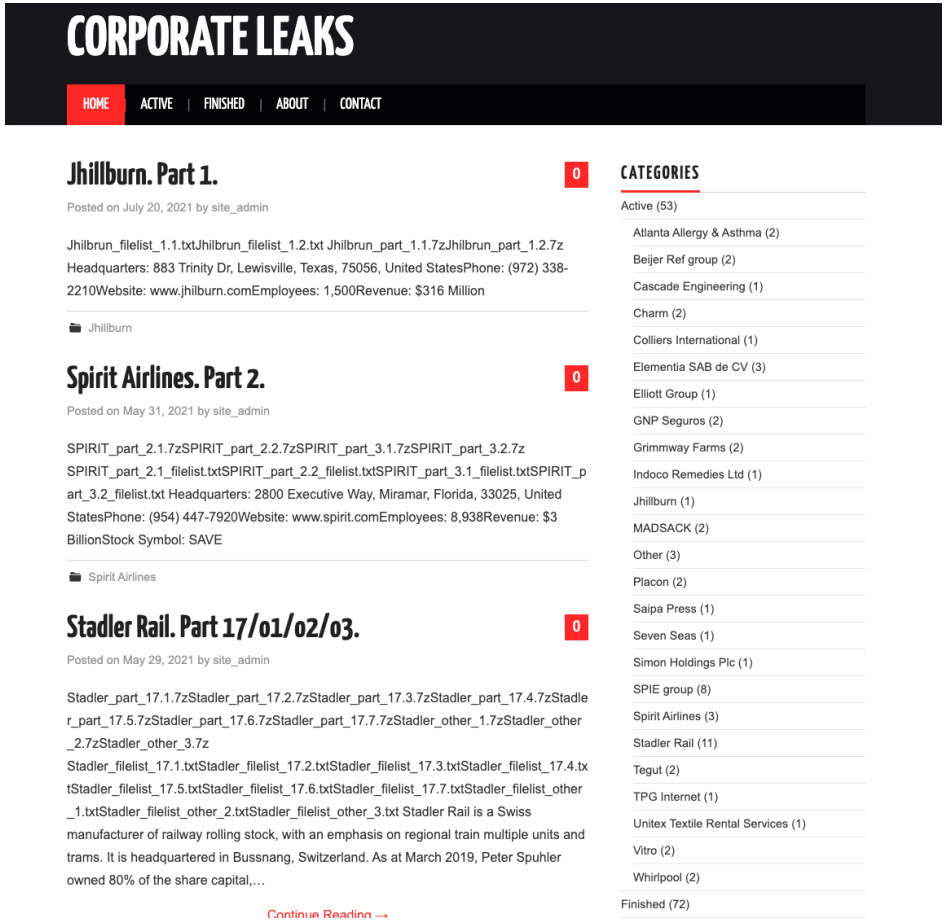




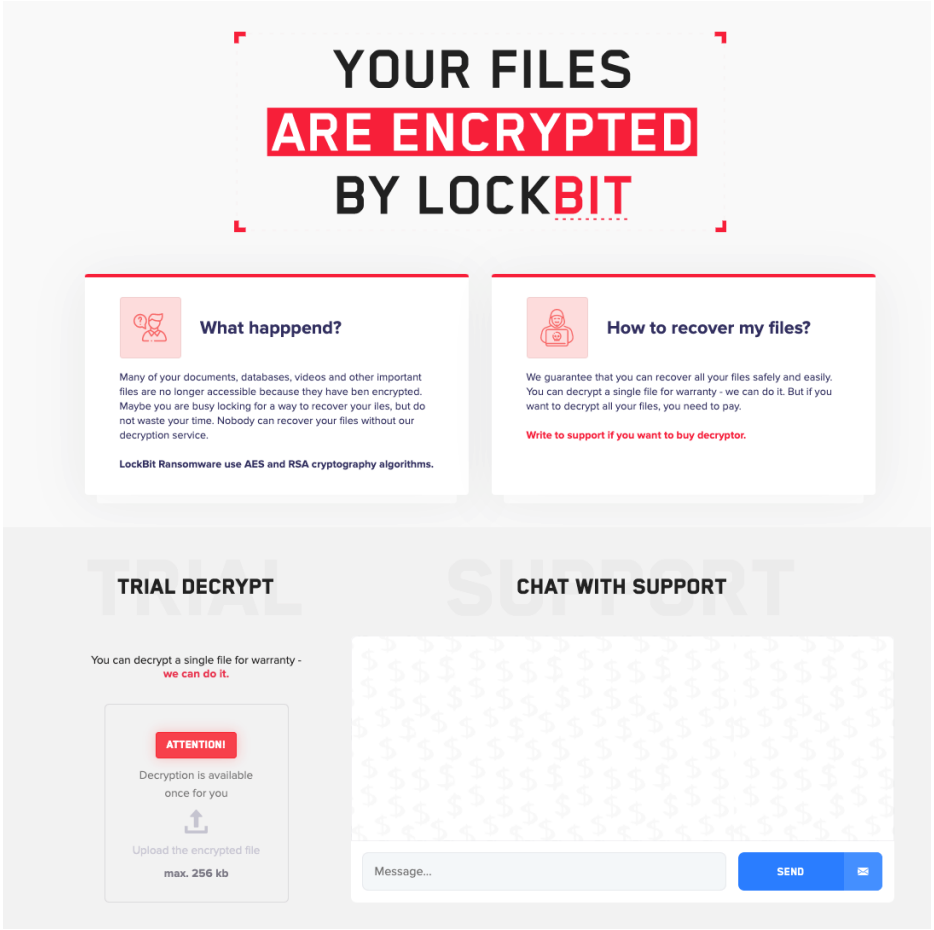
© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

Not just ransomware..

- Advanced Persistent Threats;
- Breach Assessments:
  - Hafnium 0-day;
  - Kaseya VSA supply chain attack;
  - Solarwinds supply chain attack.

© 2021 Trend Micro Inc.

Check your Incident Response plan!

© 2021 Trend Micro Inc.

Incident Response process

SANS & NIST:

1. Preperation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

© 2021 Trend Micro Inc.

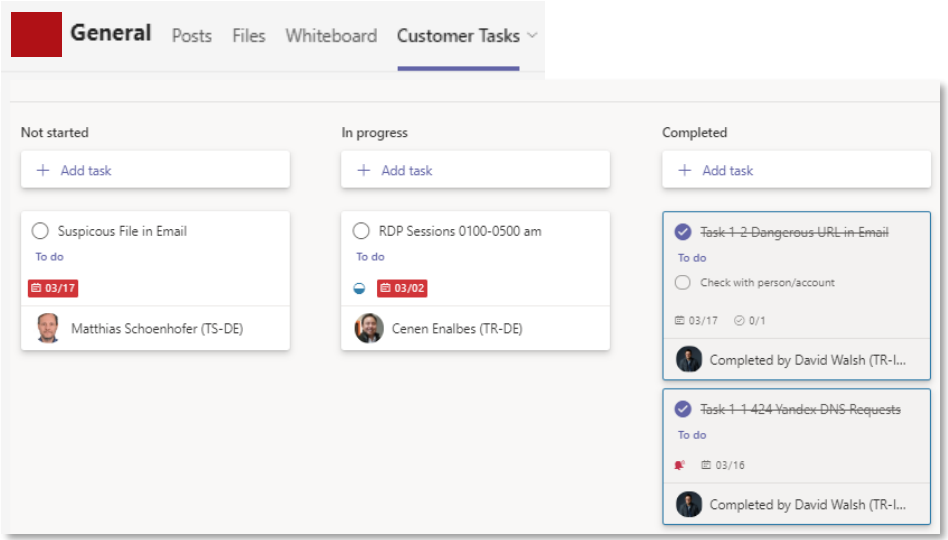
1: Preperation

- First customer call: triage.
- Setup Crisis Management Team;
- Setup Crisis Engineering Team.

Once green light: engagement starts right away.
Not limited to 9-5 business hours.

© 2021 Trend Micro Inc.

Daily Calls and Daily Reports & Tasks

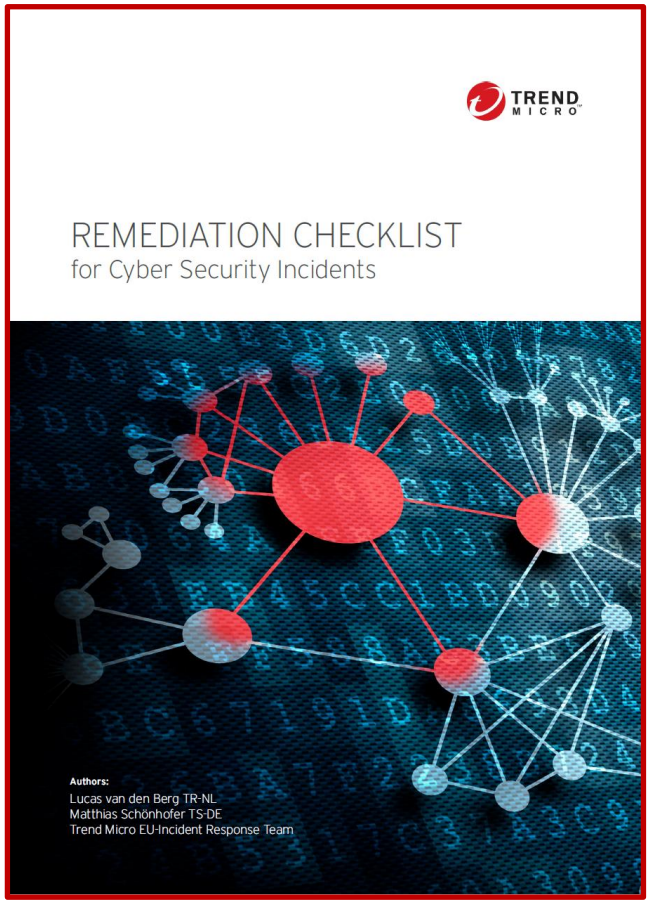


© 2021 Trend Micro Inc.

2: Identification

- Identify threats from log alerts, IDS/IPS, firewalls, and any other suspicious activity occurring on the network.
- Configure emergency containment policy’s.

© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

Gain visibility.
Harden endpoints and servers.
Isolate infected domains.

© 2021 Trend Micro Inc.

© 2021 Trend Micro Inc.

3 & 4: Containment and Eradication

1. DDI monitoring;
2. Host based forensics:
    1. Everything you do on a Windows machine is logged.

© 2021 Trend Micro Inc.

Host based forensics

"Evidence of..." categories:

- User Communications
- File Download
- Program Execution
- File Opening/Creation
- File Knowledge
- Physical Location
- USB Key Usage
- Account Usage
- Browser Usage

© 2021 Trend Micro Inc.

99% of Forensic Analysis Focuses on 1% of the Data.

© 2021 Trend Micro Inc.

Host based forensics

1. Host based forensics:
    1. Image RAM;
    2. Check for disk encryption;
    3. Create triage disk image;
    4. Analyze triage image;
    5. Image entire hard drive.

© 2021 Trend Micro Inc.

Host based forensics: RAM

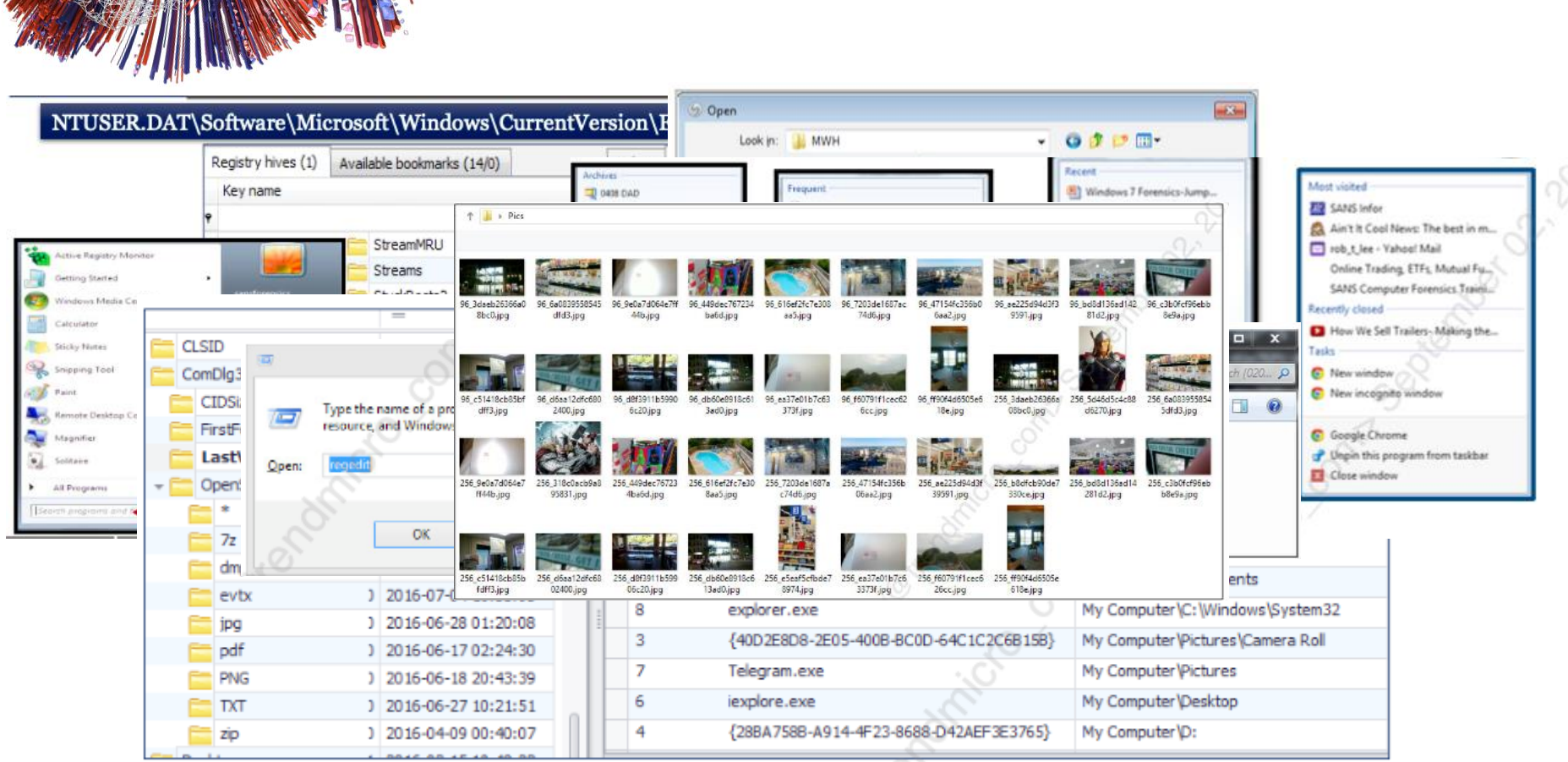
- Volatile data;
- Processes;
- Open files, registry keys and devices;
- Encryption keys and passwords;
- Network connections;
- **Memory-only exploits / rootkits.**

© 2021 Trend Micro Inc.

Host based forensics: Disk Analysis

- Data steam carving (chats);
- File carving (deleted files);
- Registry forensics:
  - System and user hives.

© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

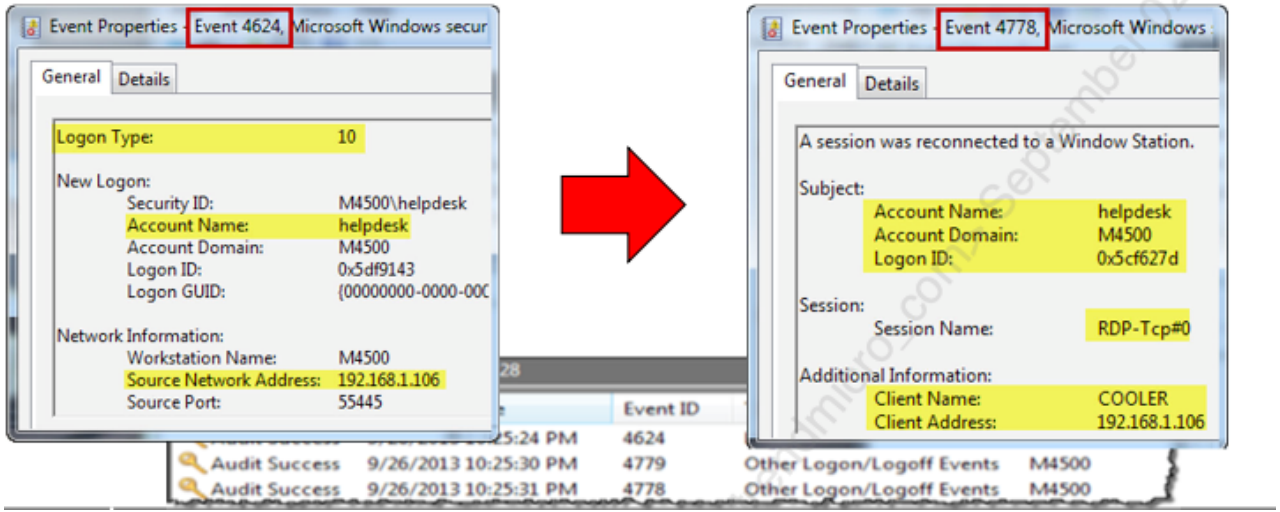
Tracking account usage

Event ID 4778: Session Reconnect

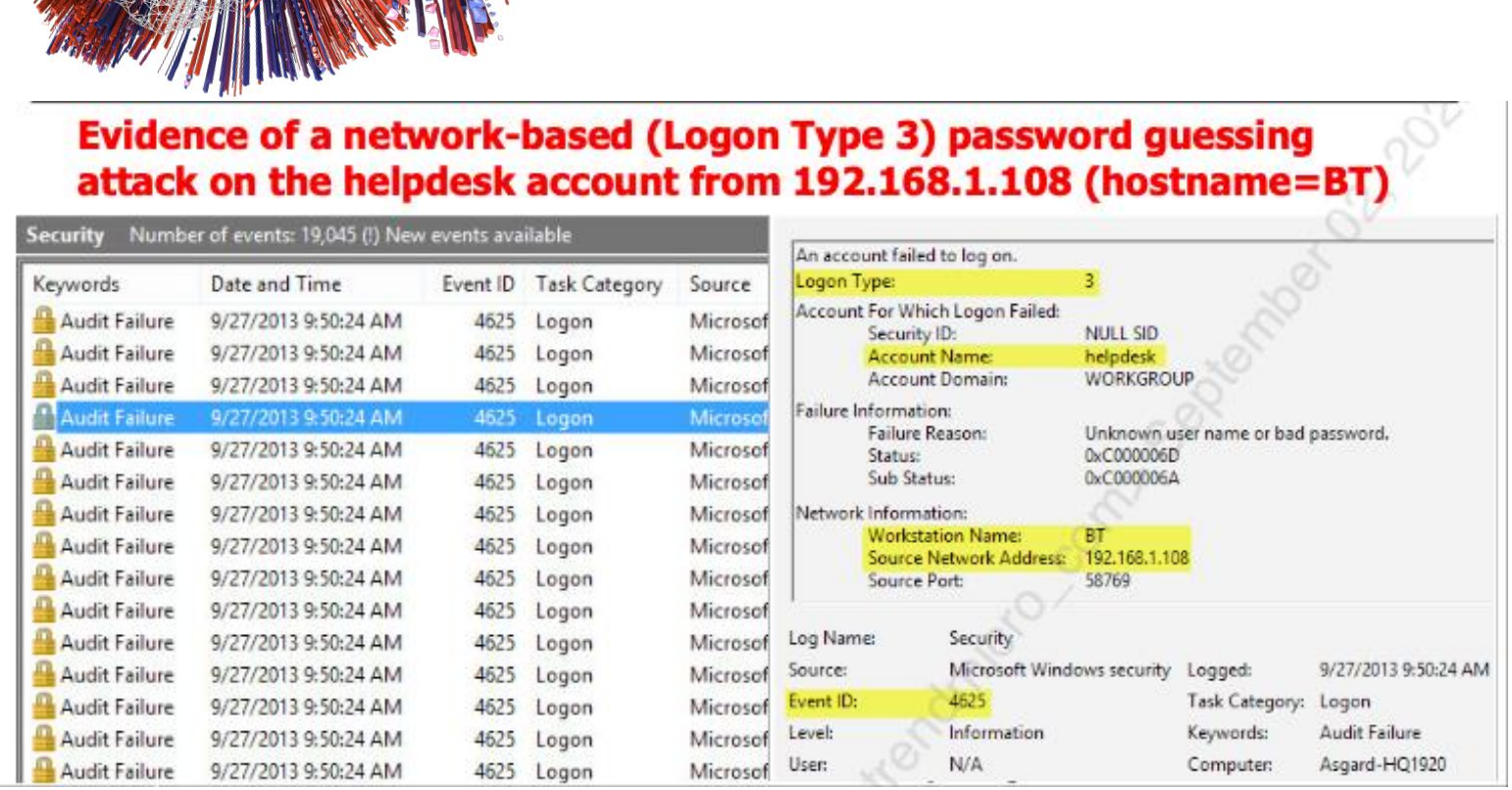
Event ID 4779: Session Disconnect

Logon Type Code	Explanation
2	Logon via console (keyboard, server KVM, or virtual client)
3	Network logon
4	Batch logon – often used by Scheduled Tasks
5	Windows Service logon
7	Credentials used to lock or unlock screen; RDP session reconnect
8	Network logon sending credentials in cleartext
9	Different credentials used than logged-on user — RunAs /netonly
10	Remote interactive logon (Remote Desktop Protocol)
11	Cached credentials used to logon – system likely offline from DC
12	Cached Remote Interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

Evidence of a Type 10 Logon (RDP) to M4500 using the helpdesk account from a system with hostname COOLER (192.168.1.106)



© 2021 Trend Micro Inc.



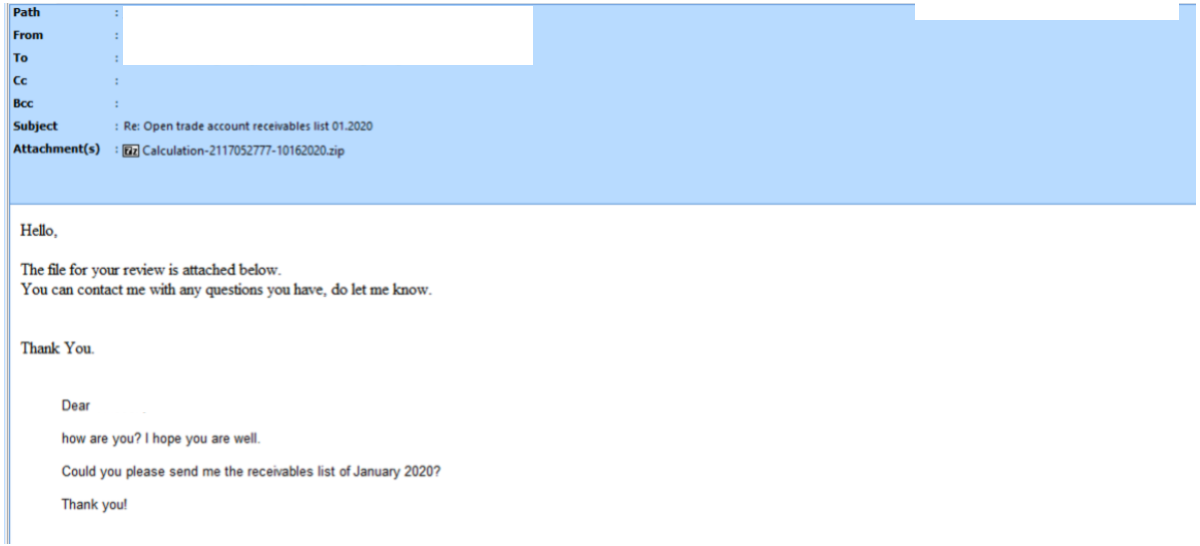
4625: An account failed to log on

© 2021 Trend Micro Inc.

Date and Time	Local Host	Description	Type	User Account	Source Host	Remote Host	Source of Evidence
	2054	%20BETEILIGUNGEN/Löschen/Calculation-2117052777-10162020.zip opened					ShellBags
	2054	al\Microsoft\Windows\Safety\shell\remote\script_570668359200864445745129364842934738 40.rel.v log file updated, indication of shell command execution perhaps					
	2054	er/Verwaltung/(2)%20BETEILIGUNGEN/Löschen/Calculation-2117052777-10162020/Calculation-2117052777-10162020.xlsb opened					WEBHIST
	2054	\Nivadalo directory created					Filesystem
	2054	Nivadalo\nosto.exe executed					AppCompatCache Registry Entry, normally when file is
	2054	Nivadalo\nosto.exe dropped					Filesystem, not present anymnore but able to get from
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg\efawlynp.dat dropped					Filesystem
	2054	\AppData\Local\Temp\~efawlynp.tmp created					Filesystem
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg directory created					Filesystem
	2054	O\sxhxzwgoainecwlnxcdw.exe executed					AppCompatCache Registry Entry, not present anymore
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg\lbebuiblq.hwt file created					Filesystem
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg\u - directory created					Filesystem
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg\aorylr.uqi					Filesystem
	2054	hxxp://vgspaqlik/QvAJAXZfc/opendoc[.]htm?document=prod_71%5Ccockpit%5Cvertrieb%5Csales[.]qvw&lang=en-US&host=QVS%40vgspaqlik (QlikView)					
	2054	\AppData\Roaming\Microsoft\Tcarpdrkiyg\cgnjjgta.ppr					Filesystem
	2054	Docs Viewer Chrome Extension used, perhaps to view the file (https://chrome.google.com/webstore/detail/docs-viewer/eomobieikegbkbaoobfcjjckhfkdgdlb)					
	2054	dwmrcs Strings: ["\r\nListening on port: 6129\r\nProtocol Family: AF_INET6\r\nListening on port: 6129\r\nProtocol Family: AF_INET\r\nService: C:\\WINDOWS\\dwrcs\\DWRCS.EXE -service					Application.evtx
	2054	<Data Name="Command">DWRCST.exe</Data>					Microsoft-Windows-Shell-Core%4Operational.evtx
	2054	[9707 / 0x25eb] Strings: ['efawlynp.exe"'], <Data Name="Command">efawlynp.exe"</Data> (ShellTraceId_Explorer_ExecutingFromRunKey_Info), most likely after user logged in via RDP					Microsoft-Windows-Shell-Core%4Operational.evtx
	2054	//T:/User/Verwaltung/(2)%20BETEILIGUNGEN/Löschen/Calculation-2117052777-10162020.zip Accessed again					
	2054	Manual scan Trend Micro Apex One started					MSIE WebCache container record
	2054	https://www.virustotal.com/gui/ - Virus total accessed to submit the file					
	2054	C:\Users\JKO\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\6SXBX03M\Calculation-2117052777-10162020.zip					
	2054	https://get.teamviewer.com, _ _ (TeamViewer)					Chrome History
	2054	C:\Temp\JKO\Downloads\TeamViewerQS.exe					AppCompatCache Registry Entry
	2054	User mks activity, login?					Filesystem
	2054	C:\Users\JKO\lqzqlszgrabhlkcoclewcwzwhhyirx.exe					AppCompatCache Registry Entry
	2054	C:\Users\JKO\kotrvidfntbignzjvcqrbyjjkq.exe					AppCompatCache Registry Entry
	2054	C:\Users\JKO\gljxowzpxsrfmxmctpfys.exe					AppCompatCache Registry Entry
	2054	C:\Users\JKO\potwgoaincklcoateropr.exe					AppCompatCache Registry Entry
	2054	C:\Users\JKO\yqcmnzhzsxeejrjplfrcumjhqf.exe					AppCompatCache Registry Entry
	2054	<Data Name="TaskName">\G2MUpdateTask-S-1-5-21-854245398-1220945662-1417001333-6361</Data>					Microsoft-Windows-TaskScheduler%4Operational.evtx
	2054	MAC of \Users\JKO\AppData\Roaming\Microsoft\Tcarpdrkiyg\aorylr.uqi					Filesystem
	2054	MAC of \Users\JKO\AppData\Roaming\Microsoft\Tcarpdrkiyg\lbebuiblq.hwt					Filesystem
	2054	C:\Users\JKO\AppData\Roaming\Microsoft\Tcarpdrkiyg\efawlynp.exe - executed, some RDP and scheduled task events around it					AppCompatCache Registry Entry
	2054	C:\Users\JKO\yvfrrbkuajdvpjdoxjdte.exe					AppCompatCache Registry Entry
	2054	\Program Files (x86)\Trend Micro\OfficeScan Client\icrc$oth.303 - Apex Update					\Program Files (x86)\Trend Micro\OfficeScan Client\icr
	2054	C:\Users\JKO\G:\Users\JKO\efawlynp.npl dropped					Filesystem
	2054	\Users\JKO\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-854245398-1220945662-1417001333-6712\8ccb0d2a53feb026579b1111803c01e5_514c5679-e92c-4f02-a54f-1a39fd7c1b9d					Filesystem
	2054	\Program Files (x86)\Trend Micro\OfficeScan Client\Suspect\Backup\{F6A1EB94-1CA4-4A17-A649-1432BD552FE4}.48731780.qtn					Filesystem
	2054	[106 / 0x006a] Strings: ['\\{F6A1EB94-1CA4-4A17-A649-1432BD552FE4}' - scheduled task created					Event Log
	2054	Users/JKO/AppData/Roaming/Microsoft/Tcarpdrkiyg/efawlynp.exe - Startup Program added					Users/JKO/NTUSER.DAT, SOFTWARE\Microsoft\Windo
	2054	Apex kicks in again - Path hints: \Program Files (x86)\Trend Micro\OfficeScan Client\Backup\TSC_GENCLEAN_2020_10_23_11_03_22_239_035.DAT					Filesystem
	2054	MAC of \Users\JKO\AppData\Roaming\Microsoft\Tcarpdrkiyg\efawlynp.dat					Filesystem
	2054	C:\ProgramData\ntuser.pol modified					Filesystem
	2054	\Windows\Prefetch\YVFRRBKUAJDVPJDOXJDTE.EXE-224A363E.pf					Prefetch
	2054	\Windows\Prefetch\CMD.EXE-0BD30981.pf					Prefetch
	2054	\Windows\Prefetch\COMPPKGSRV.EXE-4780F0C1.pf					Prefetch
	2054	\Windows\Prefetch\FIND.EXE-AE190082.pf					Prefetch
	2054	\Windows\Prefetch\NET1.EXE-509326A5.pf					Prefetch
	2054	\Windows\Prefetch\POWERSHELL.EXE-AE8EDC9B.pf					Prefetch
	2054						

Patient zero (RCA)

“On the 19th of October 2020 at 11:19 UTC (13:19 in Germany) user received an email with malicious attachment Calculation-2117052777-10162020.zip."



Path :
From :
To :
Cc :
Bcc :
Subject : Re: Open trade account receivables list 01.2020
Attachment(s) : Calculation-2117052777-10162020.zip

Hello,

The file for your review is attached below.
You can contact me with any questions you have, do let me know.

Thank You.

Dear

how are you? I hope you are well.

Could you please send me the receivables list of January 2020?

Thank you!

© 2021 Trend Micro Inc.

User opened the attachment, but content did not display on the screen and user thought that either the attachment is corrupt, or they do not have appropriate software to open it.

Therefore, they forwarded the email to two other users asking to see if they could open it.

User XXX received the email and tried to open the attachment on host XXX on the XXth of October. They encountered the same issue and submitted request to IT asking for help.

IT investigated and found nothing wrong.

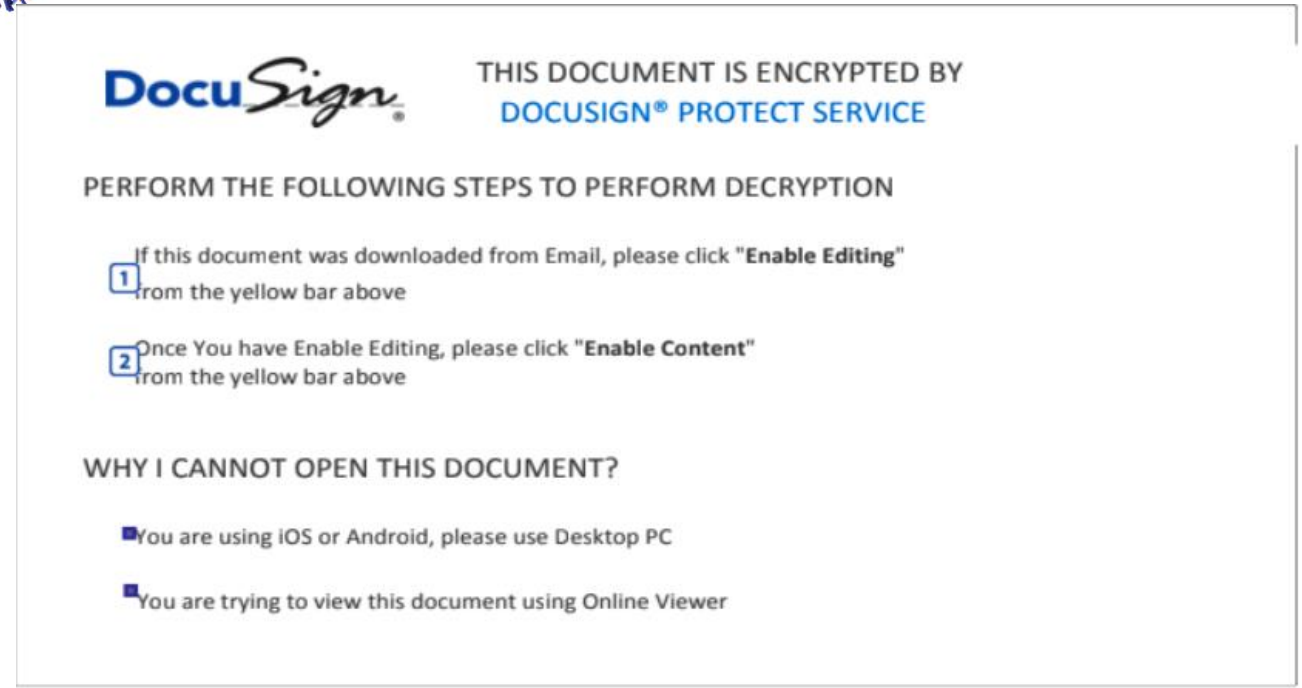
© 2021 Trend Micro Inc.

The attachment zip file contains XLSB file Calculation-2117052777-10162020.xlsb.

Attachment Name	Subject	Size (KB)
Calculation-2117052777-101...	Re: Open trade account rec...	21

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
Calculation-2117052777-10162020.xlsb	XLSB File	21 KB	No	27 KB	20%	i21

© 2021 Trend Micro Inc.



© 2021 Trend Micro Inc.

ExifTool File Metadata

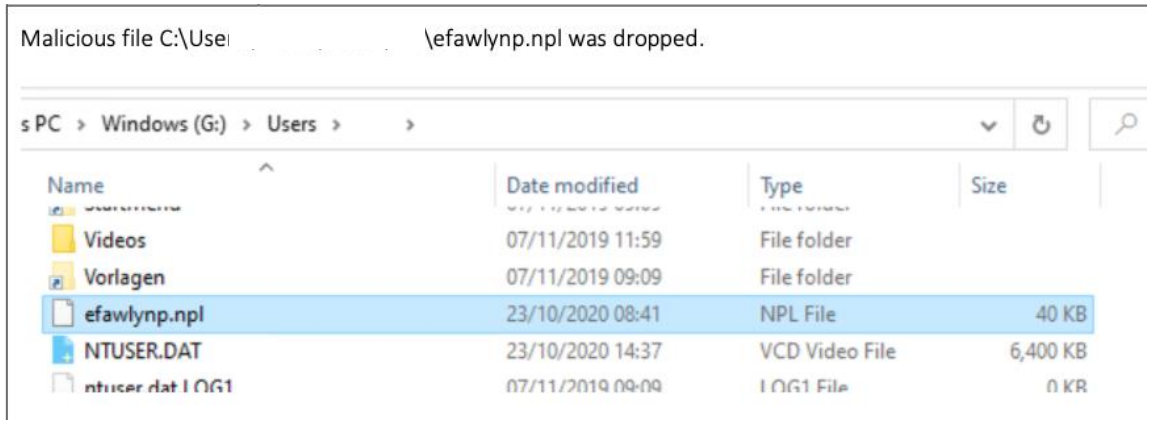
SharedDoc	No
HyperlinksChanged	No
TitlesOfParts	DocuSign®, Лист1, Лист2, Лист3, Лист4
LinksUpToDate	No
LastModifiedBy	Пользователь Windows
HeadingPairs	Листы, 4, Макросы Excel 4.0, 1
ZipFileName	[Content_Types].xml
CreateDate	2006:09:16 00:00:00Z
ZipRequiredVersion	20
ModifyDate	2020:10:19 10:15:21Z
ZipCRC	0x9f2bf8a2
ZipBitFlag	0x0006
Application	Microsoft Excel
ScaleCrop	No
MIMEType	application/vnd.ms-excel.sheet.binary.macroEnabled
FileType	XLSB
AppVersion	14.03
ZipUncompressedSize	2406
ZipCompressedSize	514
DocSecurity	None
ZipModifyDate	1980:01:01 00:00:00
Creator	Admin
ZipCompression	Deflated
FileTypeExtension	xlsb

© 2021 Trend Micro Inc.

Investigation and timeline

Date and Time (UTC)	Event Description / Comments
20/10/2020 06:07:55	
User saved the attachment to T:/I öschen/Calculation-2117052777-10162020.zip and opened it	
20/10/2020 06:09:09	
File (\\\ 20BETEILIGUNGEN/Löschen/Calculation-2117052777-10162020/Calculation-2117052777-10162020.xlsb in ZIP archive was opened. At the same time log file at dows\Safety\shell\remote\ script_5706683592008644457451293648429347384O.rel.v was updated which indicates of shell command execution	
20/10/2020 06:09:10	› directory was created
20/10/2020 06:09:14	C: nosto.exe was dropped and executed
20/10/2020 06:09:30	\Users\. ning\Microsoft\Tcarpdrkiyg directory created
20/10/2020 06:09:30	\Users\ ming\Microsoft\Tcarpdrkiyg\efawlynp.dat (encrypted file) was dropped
20/10/2020 06:09:30	\AppData\Local\Temp\~efawlynp.tmp file created
20/10/2020 06:26:45	
C:\ sxhxzwgoainecwlnxcdw.exe file was executed. At this stage it is likely that attacker was on the host. It is unknown when the file sxhxzwgoainecwlnxcdw.exe was created on the computer. Files with the same path and similar name are executed on the host during of October periodically (refer to Investigation_Overview.xlsx for details). These files were later detected as QAKBOT backdoor.	

© 2021 Trend Micro Inc.



The file efawlynp.npl was executed straight away. It is likely that it was executed using scheduled task.

© 2021 Trend Micro Inc.

It drops three BAT files in %ALLUSERSPROFILE%, all detected by Trend Micro as Trojan.BAT.QAKBOT.SM1:

Characteristic	Significance	Details
Drops known malware	■■■	Source: ATSE Detection Name: Trojan.BAT.QAKBOT.SM1 File Name: FUXvRI3s.bat SHA1: 9942A3080CE1F32857FD95437C53D2BB28DA8F3B Engine Version: 12.500.1008 Malware Pattern Version: 16.657.92
Drops known malware	■■■	Source: ATSE Detection Name: Trojan.BAT.QAKBOT.SM1 File Name: 1k79VxVa.bat SHA1: 437FC21129E329E6F776D602F0EBCD67DA338ACE Engine Version: 12.500.1008 Malware Pattern Version: 16.657.92
Drops known malware	■■■	Source: ATSE Detection Name: Trojan.BAT.QAKBOT.SM1 File Name: rFPIVL7Z.bat SHA1: 05C79D0A239175841F6DA6982C5909FC7768F443 Engine Version: 12.500.1008 Malware Pattern Version: 16.657.92

It also adds the following scheduled tasks:

Characteristic	Significance	Details
Adds scheduled task to automatically run at startup	■■□	1k79VxVa /TR "cmd /c \"start /min %ALLUSERSPROFILE%\1k79VxVa.bat\"" /ST
Adds scheduled task to automatically run at startup	■□□	FUXvRI3s /TR "cmd /c \"start /min %ALLUSERSPROFILE%\FUXvRI3s.bat\"" /ST
Adds scheduled task to automatically run at startup	■□□	rFPIVL7Z /TR "cmd /c \"start /min %ALLUSERSPROFILE%\rFPIVL7Z.bat\"" /ST

© 2021 Trend Micro Inc.

Qakbot

- Previously distributed by Emotet, but can appear through malspam email campaigns;
- Can also self-spread using an SMB brute force module that contains a list of commonly used passwords;
- Sells access to ransomware affiliate (Egregor / REvil/Sodinokibi / Maze);
- JBS ransomware attack in Brazil ($11 million ransom payment).

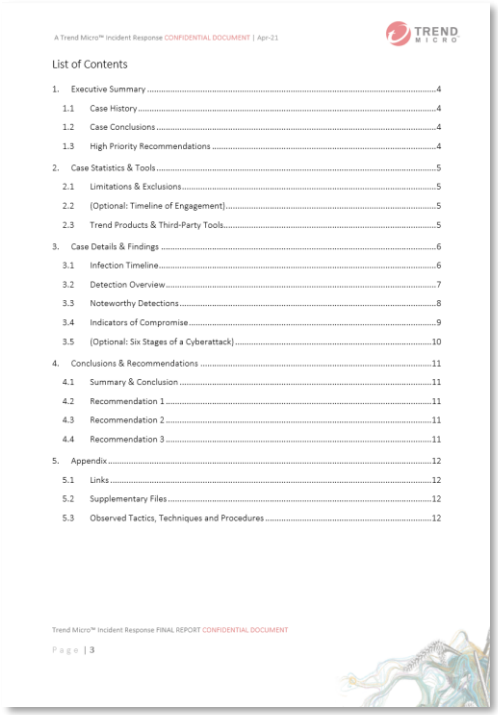
© 2021 Trend Micro Inc.

5: Lessons Learned

1. Setup an Incident Response Plan;
2. Test your Incident Response Plan;
3. Harden endpoints;
4. Harden e-mail systems;
5. Harden server environment;
6. Gain visibility on network;
7. Train users on security awareness.

© 2021 Trend Micro Inc.

Final Call and Final Report



© 2021 Trend Micro Inc.

incident_response@trendmicro.com

© 2021 Trend Micro Inc.

TREND MICRO™

THE ART OF CYBERSECURITY

The global shift of Trend Micro customers from on-premises to SaaS-based security. **Created with real data by artist Brendan Dawes.**