
HORNETSECURITY

How Emotet decomposes a company

Dr. Yvonne Bernard

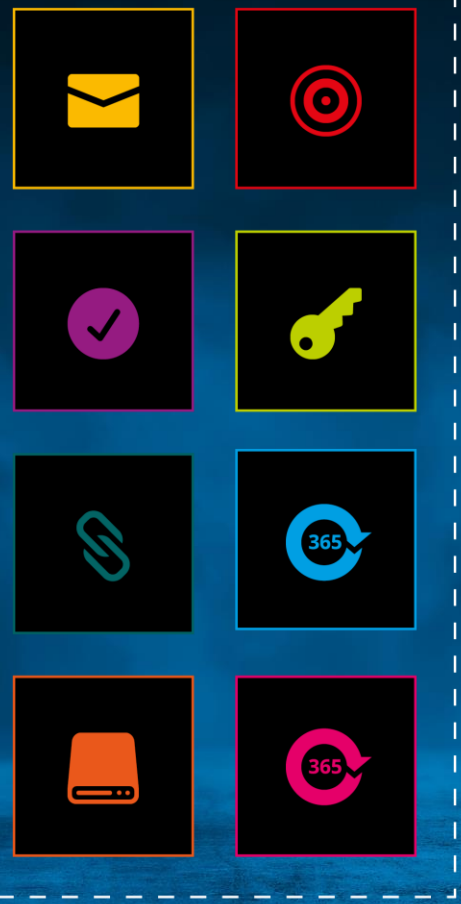
HORNETSECURITY

ABOUT HORNETSECURITY

HORNETSECURITY

CONTROL PANEL

- Easily manage clients and partners
- Multi-tenant capability
- Be in control of 100 % of your email traffic



SPAM FILTER

- Deep scanning of email traffic by highly effective filters
- Encryption of data traffic and advanced routing of emails
- Better than 99.9 % spam and 99.99 % virus recognition

EMAIL CONTINUITY

- Continuous availability of email traffic during an email server outage
- Rolling backup of email traffic for the past 3 months
- Fully automated process

EMAIL SIGNATURE AND DISCLAIMER

- Consistent email signatures automatically populated with personalized information
- Active directory integration including group-based assignment
- Easiest implementation and import function for HTML disclaimer with WYSIWYG editor

EMAIL ARCHIVING

- Fully automated audit compliant email archiving
- Mobile usage and Outlook plug-in
- Full-text search for easy retrieval of emails and attachments

ADVANCED THREAT PROTECTION

- Protection against complex and highly evolved threats
- Detection of Ransomware, CEO Fraud and Spearphishing attacks
- Sandboxing and highly innovative forensic analysis engines

EMAIL ENCRYPTION

- Fully automated, policy-based encryption of emails
- Compliance, transparency and control
- Automated certificate handling

365 TOTAL PROTECTION BUSINESS

- Seamlessly integrated Company Security Management for Office 365
- Compliance, email and data security by default
- Company-wide consistent appearance through email signature features

365 TOTAL PROTECTION ENTERPRISE

- Full-featured Security & Compliance Suite for Office 365
- Extended functionality and advanced protection mechanisms
- Global Security Dashboard: Real-time attack overview and comprehensive reporting

HOW EMOTET DECOMPOSES A COMPANY

Source: Heise.de

16.11.2018 14:47 Uhr

Fürstenfeldbruck: Malware legt Klinikums-IT komplett lahm

Im bayerischen Fürstenfeldbruck muss die örtliche Klinik seit Tagen fast komplett ohne Computer auskommen; verantwortlich ist Malware.

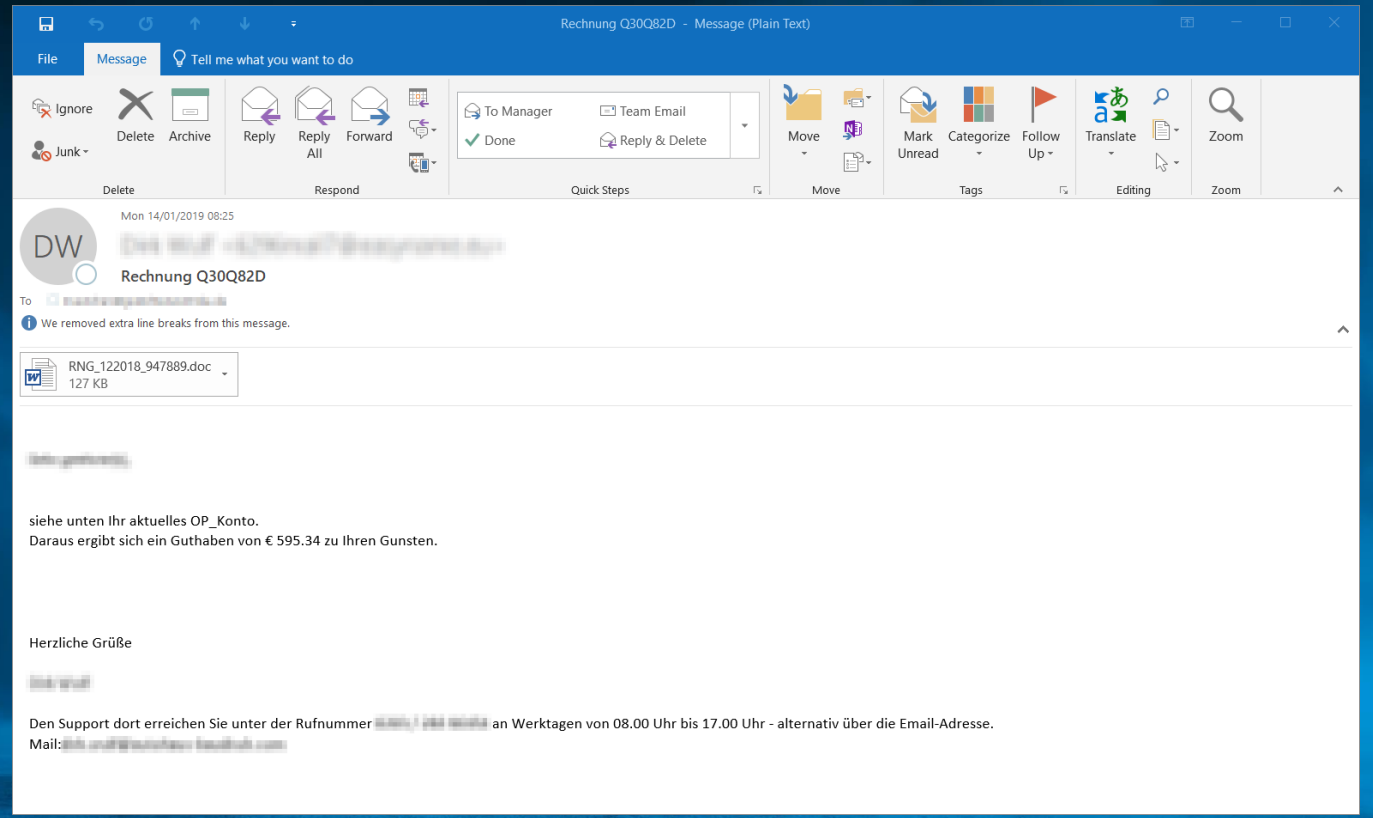
Von **Martin Holland** 762

Das Klinikum Fürstenfeldbruck (Bild: Klinikum FFB)

Das Klinikum Fürstenfeldbruck in Bayern muss seit einer Woche ohne Computer auskommen, nachdem offenbar ein per Mail empfangener Trojaner die IT-Systeme infiziert hat. Das meldet der *Münchner Merkur* unter Berufung auf Verantwortliche des Krankenhauses in der Kreisstadt westlich von München. Noch immer werden demnach fast alle der 450 vorhandenen Computer überprüft und die Angelegenheiten des Hauses müssen weitgehend ohne IT-Unterstützung erledigt werden. Erst in den kommenden Tagen sollten alle Geräte wieder funktionieren.

„These are cases in which one hundred percent of the network's servers and computers have collapsed", said a BSI spokesman. (FAZ, 7.12.18)

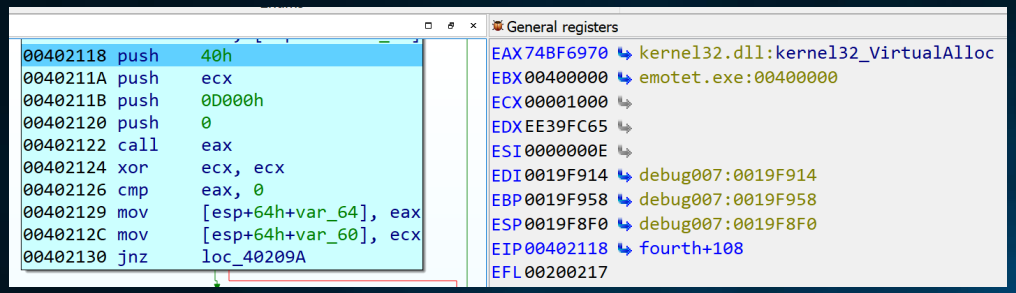
EMOTET KILL-CHAIN



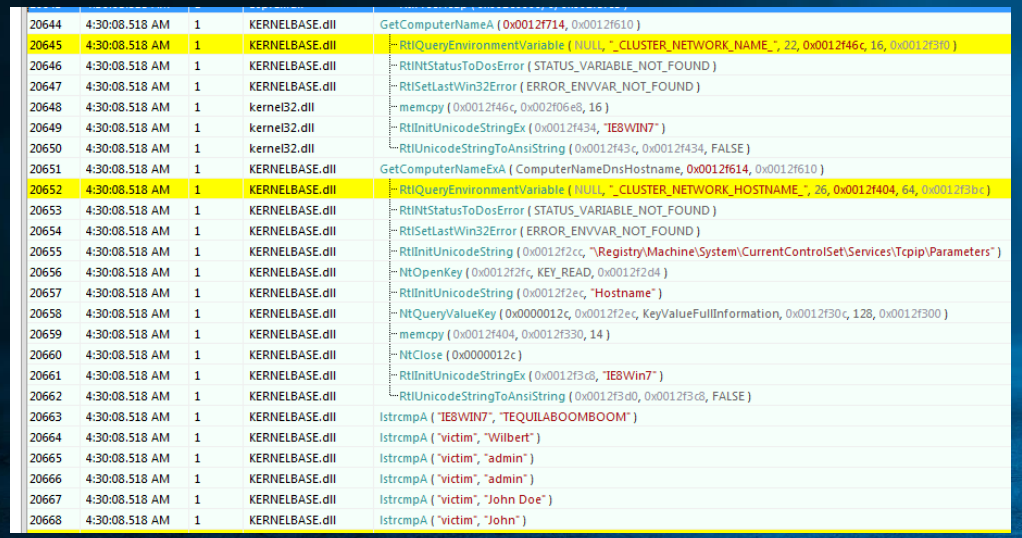
ATTEMPTS TO AVOID SANDBOX ANALYSIS

HORNETSECURITY

- Complicate static analysis:



- Checking for familiar names:

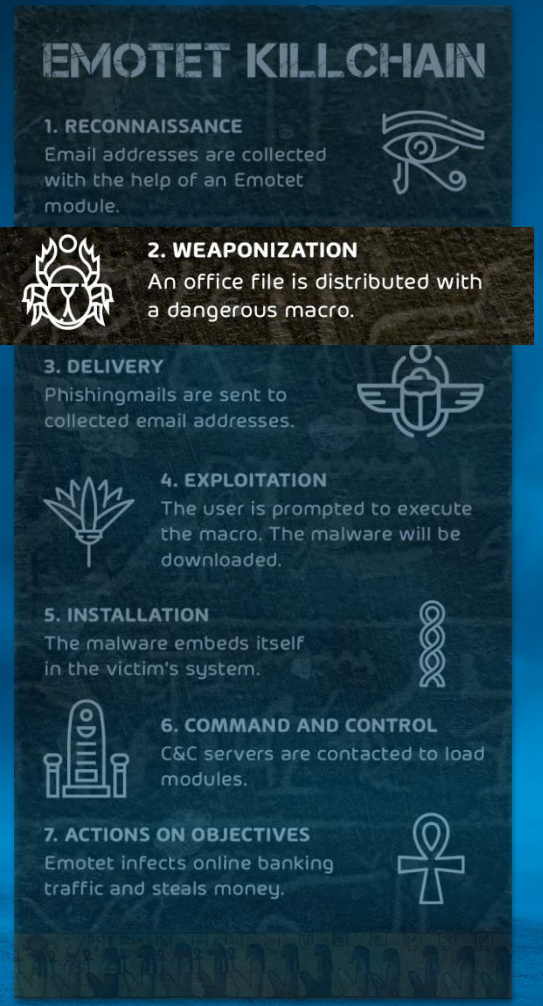


ATTEMPTS TO AVOID SANDBOX ANALYSIS

HORNETSECURITY

- Verification if known sandbox files exist:

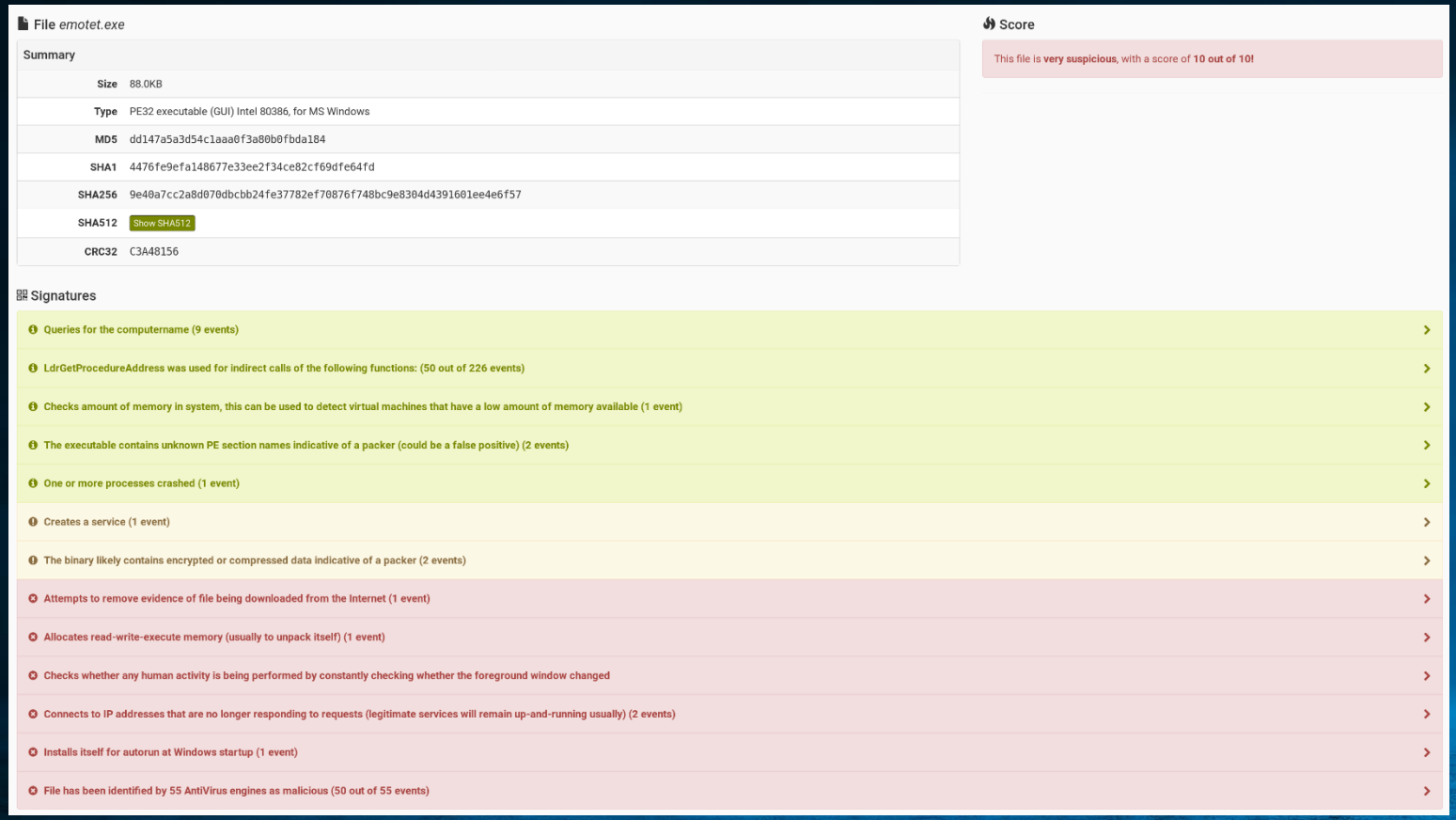
20669	4:30:08.518 AM	1	KERNELBASE.dll	CreateFileA ("C:\email.doc", GENERIC_READ, 0, NULL, OPEN_EXISTING, 0, NULL)
20670	4:30:08.518 AM	1	kernel32.dll	RtlInitAnsiStringEx (0x0012f448, "C:\email.doc")
20671	4:30:08.518 AM	1	KERNELBASE.dll	RtlAnsiStringToUnicodeString (0x0012f460, 0x0012f448, TRUE)
20672	4:30:08.518 AM	1	kernel32.dll	RtlInitUnicodeStringEx (0x0012f430, "C:\email.doc")
20673	4:30:08.518 AM	1	kernel32.dll	RtlIsDosDeviceName_U ("C:\email.doc")
20674	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea6c, TRUE)
20675	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea74, TRUE)
20676	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea7c, TRUE)
20677	4:30:08.518 AM	1	KERNELBASE.dll	RtlInitUnicodeStringEx (0x0012f3e4, "C:\email.doc")
20678	4:30:08.518 AM	1	KERNELBASE.dll	RtlDosPathNameToRelativeNtPathName_U_WithStatus ("C:\email.doc", 0x0012f3e4, NULL, 0x0012f3c0)
20679	4:30:08.518 AM	1	KERNELBASE.dll	NtCreateFile (0x0012f404, FILE_READ_ATTRIBUTES | GENERIC_READ | SYNCHRONIZE, 0x0012f3a8, 0x0012f3ec, NULL, 0, 0, FILE_OPEN, FILE_NON_DIRECTORY_FILE | FILE_SYNCHRONOUS_IO_NONALERT, NULL, 0)
20680	4:30:08.518 AM	1	KERNELBASE.dll	RtlReleaseRelativeName (0x0012f3c0)
20681	4:30:08.518 AM	1	KERNELBASE.dll	RtlFreeHeap (0x002e0000, 0, 0x003096d8)
20682	4:30:08.518 AM	1	KERNELBASE.dll	RtlFreeHeap (0x002e0000, 0, NULL)
20683	4:30:08.518 AM	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_OBJECT_NAME_NOT_FOUND)
20684	4:30:08.518 AM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_FILE_NOT_FOUND)
20685	4:30:08.518 AM	1	kernel32.dll	RtlFreeUnicodeString (0x0012f460)
20686	4:30:08.518 AM	1	KERNELBASE.dll	CloseHandle (0xffffffff)
20687	4:30:08.518 AM	1	KERNELBASE.dll	NtClose (0xffffffff)
20688	4:30:08.518 AM	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_INVALID_HANDLE)
20689	4:30:08.518 AM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_INVALID_HANDLE)
20690	4:30:08.518 AM	1	KERNELBASE.dll	CreateFileA ("C:\a\foobar.bmp", GENERIC_READ, 0, NULL, OPEN_EXISTING, 0, NULL)
20691	4:30:08.518 AM	1	kernel32.dll	RtlInitAnsiStringEx (0x0012f448, "C:\a\foobar.bmp")
20692	4:30:08.518 AM	1	KERNELBASE.dll	RtlAnsiStringToUnicodeString (0x0012f460, 0x0012f448, TRUE)
20693	4:30:08.518 AM	1	kernel32.dll	RtlInitUnicodeStringEx (0x0012f430, "C:\a\foobar.bmp")
20694	4:30:08.518 AM	1	kernel32.dll	RtlIsDosDeviceName_U ("C:\a\foobar.bmp")
20695	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea6c, TRUE)
20696	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea74, TRUE)
20697	4:30:08.518 AM	1	kernel32.dll	RtlEqualUnicodeString (0x0012f3fc, 0x7606ea7c, TRUE)
20698	4:30:08.518 AM	1	KERNELBASE.dll	RtlInitUnicodeStringEx (0x0012f3e4, "C:\a\foobar.bmp")
20699	4:30:08.518 AM	1	KERNELBASE.dll	RtlDosPathNameToRelativeNtPathName_U_WithStatus ("C:\a\foobar.bmp", 0x0012f3e4, NULL, 0x0012f3c0)
20700	4:30:08.518 AM	1	KERNELBASE.dll	NtCreateFile (0x0012f404, FILE_READ_ATTRIBUTES | GENERIC_READ | SYNCHRONIZE, 0x0012f3a8, 0x0012f3ec, NULL, 0, 0, FILE_OPEN, FILE_NON_DIRECTORY_FILE | FILE_SYNCHRONOUS_IO_NONALERT, NULL, 0)
20701	4:30:08.518 AM	1	KERNELBASE.dll	RtlReleaseRelativeName (0x0012f3c0)
20702	4:30:08.518 AM	1	KERNELBASE.dll	RtlFreeHeap (0x002e0000, 0, 0x003096d8)
20703	4:30:08.518 AM	1	KERNELBASE.dll	RtlFreeHeap (0x002e0000, 0, NULL)
20704	4:30:08.518 AM	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_OBJECT_PATH_NOT_FOUND)
20705	4:30:08.518 AM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_PATH_NOT_FOUND)
20706	4:30:08.518 AM	1	kernel32.dll	RtlFreeUnicodeString (0x0012f460)
20707	4:30:08.518 AM	1	KERNELBASE.dll	CloseHandle (0xffffffff)
20708	4:30:08.518 AM	1	KERNELBASE.dll	NtClose (0xffffffff)
20709	4:30:08.518 AM	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_INVALID_HANDLE)
20710	4:30:08.518 AM	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_INVALID_HANDLE)



ATTEMPTS TO AVOID SANDBOX ANALYSIS

HORNETSECURITY

- Not with us ☺



File *emotet.exe*

Summary

Size	88.0KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	dd147a5a3d54c1aaa0f3a80b0fbda184
SHA1	4476fe9efa148677e33ee2f34ce82cf69dfe64fd
SHA256	9e40a7cc2a8d070dbcbb24fe37782ef70876f748bc9e8304d4391601ee4e6f57
SHA512	Show SHA512
CRC32	C3A48156

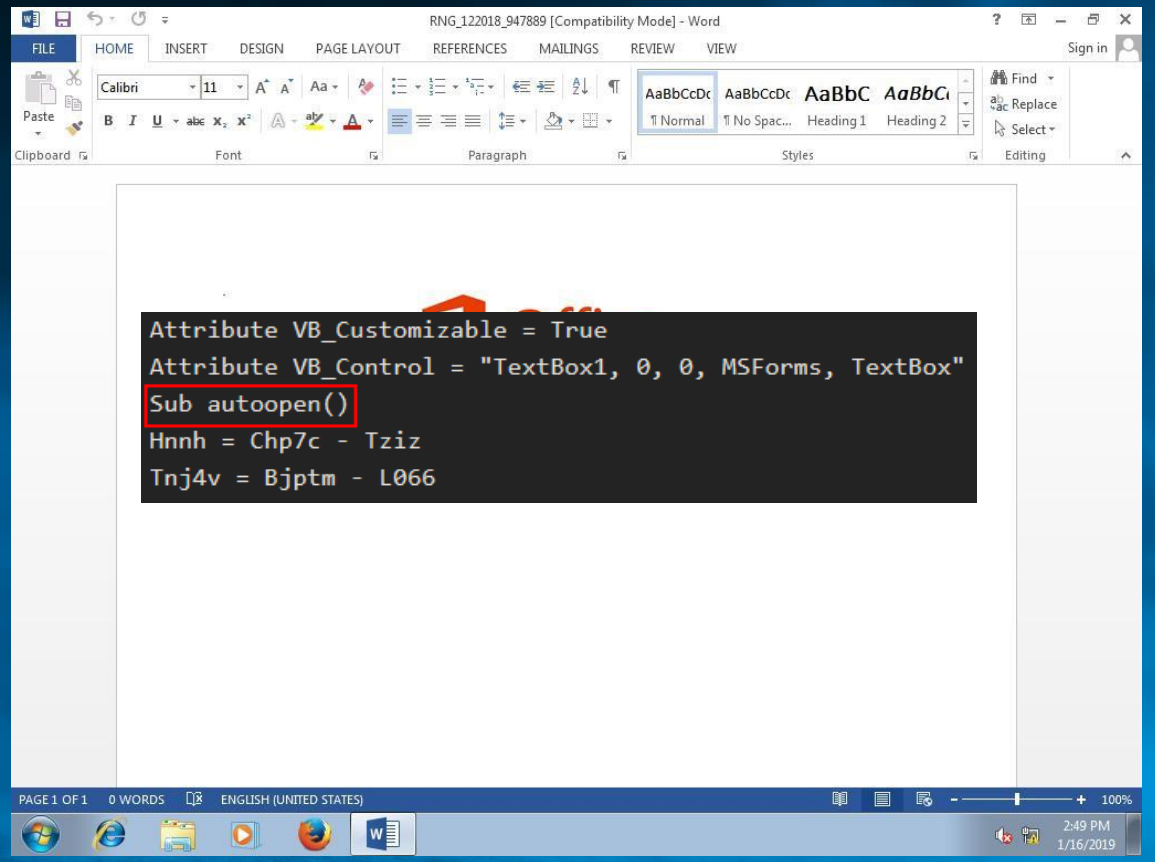
Score

This file is **very suspicious**, with a score of **10 out of 10!**

Signatures

- Queries for the computername (9 events)
- LdrGetProcedureAddress was used for indirect calls of the following functions: (50 out of 226 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable contains unknown PE section names indicative of a packer (could be a false positive) (2 events)
- One or more processes crashed (1 event)
- Creates a service (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- Attempts to remove evidence of file being downloaded from the Internet (1 event)
- Allocates read-write-execute memory (usually to unpack itself) (1 event)
- Checks whether any human activity is being performed by constantly checking whether the foreground window changed
- Connects to IP addresses that are no longer responding to requests (legitimate services will remain up-and-running usually) (2 events)
- Installs itself for autorun at Windows startup (1 event)
- File has been identified by 55 AntiVirus engines as malicious (50 out of 55 events)

EMOTET KILL-CHAIN: EXPLOITATION



EMOTET KILL-CHAIN: INSTALLATION

- Emotet copies itself to another location and deletes the original file.
- Create Registry Entries:
  - HKLM\SOFTWARE\Microsoft\Tracing\infoagent_RASAPI32
  - HKLM\SOFTWARE\Microsoft\Tracing\infoagent_RASMANCS

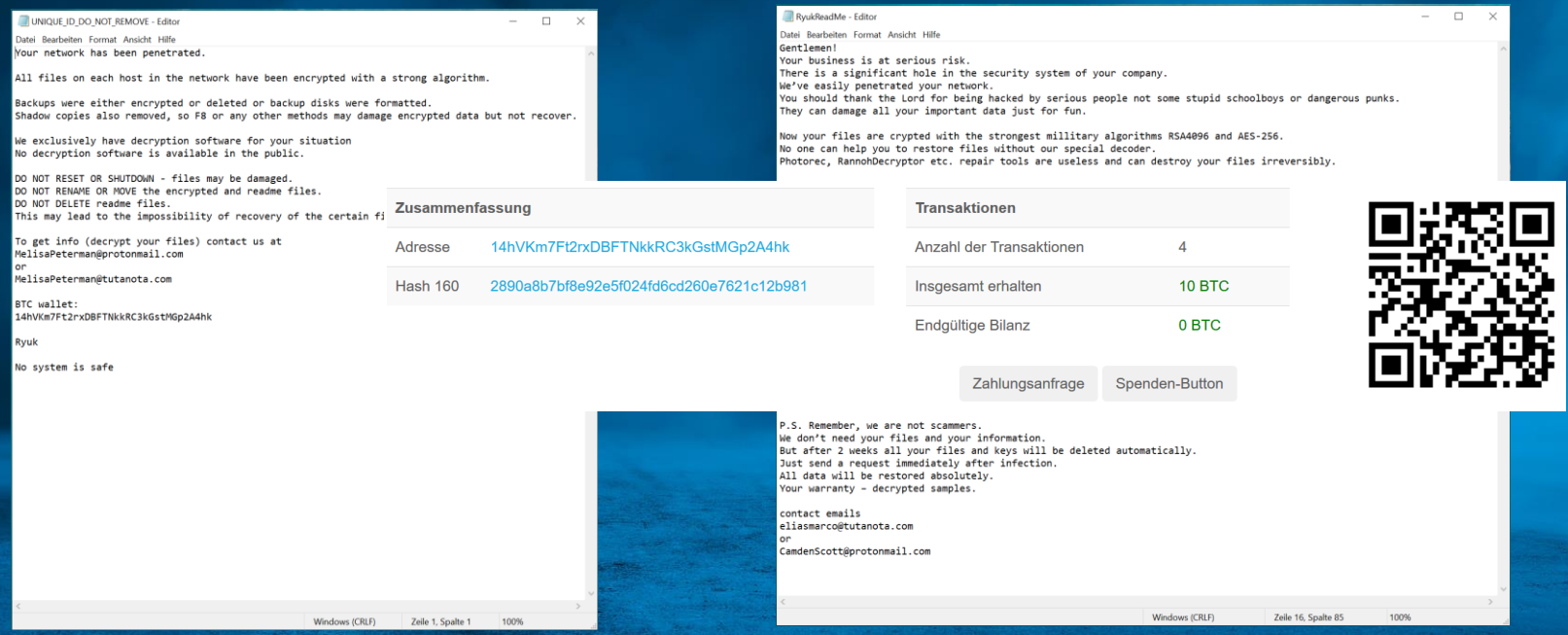
infoagent.exe	1576	0.03	4.75 MB	IE8Win7\IEUser	Web DAV Client DLL

EMOTET KILL-CHAIN: C&C

- One of the C&C servers is contacted:
  - http: //162.243.154.25:443/
  - http: //136.243.202.133:8080/
  - http: //66.234.234.36:8080/
  - http: //212.83.146.230:8080/
  - http: //209.126.105.250:8080/
  - http: //66.175.215.16:8080/
  - http: //178.254.33.12:8080/
  - http: //46.4.67.203:7080/
  - http: //147.135.209.118:443/
- Download new modules

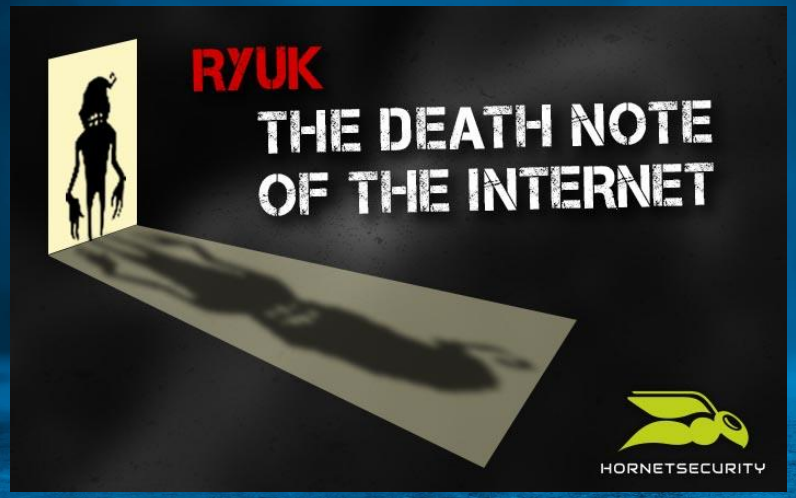
EMOTET KILL-CHAIN: ACTION!

- Origin: downloaded Banking Trojan
  - E.g. Trickbot
- New: File encryption
  - Ryuk: >2,25 Mio €
  - also deleting of backup copies
- To be continued...



FAZIT

- A single mail can stop production process for weeks
- Nevertheless: do not comply to blackmailers
- Polymorphism: Emotet changes constantly
- Reliable detection requires dynamics
- Hornetsecurity protects sustainably and proactively




HORNETSECURITY

CONTACT INFORMATION

Email: sales@hornetsecurity.com
Phone: +49 511 515 464-200
www.hornetsecurity.com