



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



## 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 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 ENCRYPTION

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

## 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



## 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

## EMAIL ARCHIVING

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



## 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



HORNETSECURITY

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.

ANZEIGE

# Frankfurter Allgemeine

Diginomics

Frankfurt am Main -1°

F.A.Z.-INDEX 📈 2.185,24 📈 +1,20 % 📈 DAX 📈 11.278,28 📈 +1,33 % 📈 EUR/USD 📈 1,1335 📈 +0,28 % 📈 DOW JONES 📈 24.553,24 ↔️

ALLE KURSE



F.A.Z. EXKLUSIV

## Cyberkriminelle erpressen Krauss Maffei

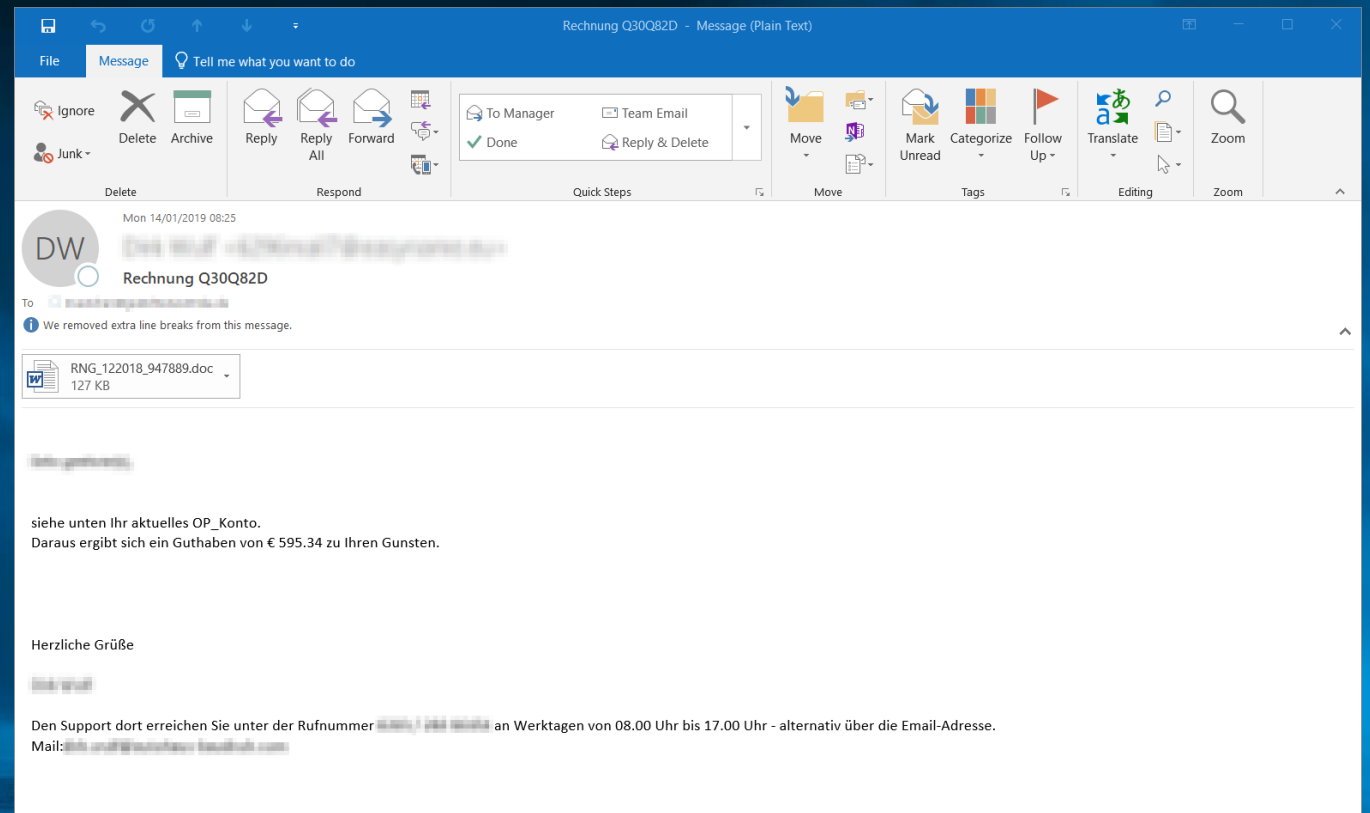
1800 Mitarbeiter hat Krauss Maffei in München. Sie mussten die Produktion drosseln, weil Hacker die Unternehmenscomputer lahmgelegt haben. Nach Informationen der F.A.Z. gibt es eine Lösegeldforderung.

„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

## EMOTET KILLCHAIN

- 1. RECONNAISSANCE**  
Email addresses are collected with the help of an Emotet module. 
- 2. WEAPONIZATION**  
An office file is distributed with a dangerous macro. 
- 3. DELIVERY**  
Phishing mails are sent to collected email addresses. 
- 4. EXPLOITATION**  
The user is prompted to execute the macro. The malware will be downloaded. 
- 5. INSTALLATION**  
The malware embeds itself in the victim's system. 
- 6. COMMAND AND CONTROL**  
C&C servers are contacted to load modules. 
- 7. ACTIONS ON OBJECTIVES**  
Emotet infects online banking traffic and steals money. 



# ATTEMPTS TO AVOID SANDBOX ANALYSIS



HORNETSECURITY

## ➤ Complicate static analysis:

```

General registers
00402118 push 40h
0040211A push ecx
0040211B push 0D000h
00402120 push 0
00402122 call eax
00402124 xor ecx, ecx
00402126 cmp eax, 0
00402129 mov [esp+64h+var_64], eax
0040212C mov [esp+64h+var_60], ecx
00402130 jnz loc_40209A

EAX 74BF6970 kernel32.dll:kernel32_VirtualAlloc
EBX 00400000 emotet.exe:00400000
ECX 00001000
EDX EE39FC65
ESI 0000000E
EDI 0019F914 debug007:0019F914
EBP 0019F958 debug007:0019F958
ESP 0019F8F0 debug007:0019F8F0
EIP 00402118 fourth+108
EFL 00200217
    
```

## ➤ Checking for familiar names:

20644	4:30:08.518 AM	1	KERNELBASE.dll	GetComputerNameA (0x0012f714, 0x0012f610)
20645	4:30:08.518 AM	1	KERNELBASE.dll	~RtlQueryEnvironmentVariable (NULL, "CLUSTER_NETWORK_NAME", 22, 0x0012f46c, 16, 0x0012f510)
20646	4:30:08.518 AM	1	KERNELBASE.dll	~RtlInitStatusToDosError (STATUS_VARIABLE_NOT_FOUND)
20647	4:30:08.518 AM	1	KERNELBASE.dll	~RtlSetLastWin32Error (ERROR_ENVVAR_NOT_FOUND)
20648	4:30:08.518 AM	1	kernel32.dll	~memcpy (0x0012f46c, 0x002f06e8, 16)
20649	4:30:08.518 AM	1	kernel32.dll	~RtlInitUnicodeStringEx (0x0012f434, "IEBWIN7")
20650	4:30:08.518 AM	1	kernel32.dll	~RtlUnicodeStringToAnsiString (0x0012f43c, 0x0012f434, FALSE)
20651	4:30:08.518 AM	1	KERNELBASE.dll	GetComputerNameExA (ComputerNameDnsHostName, 0x0012f614, 0x0012f610)
20652	4:30:08.518 AM	1	KERNELBASE.dll	~RtlQueryEnvironmentVariable (NULL, "CLUSTER_NETWORK_HOSTNAME", 26, 0x0012f404, 64, 0x0012f3bc)
20653	4:30:08.518 AM	1	KERNELBASE.dll	~RtlInitStatusToDosError (STATUS_VARIABLE_NOT_FOUND)
20654	4:30:08.518 AM	1	KERNELBASE.dll	~RtlSetLastWin32Error (ERROR_ENVVAR_NOT_FOUND)
20655	4:30:08.518 AM	1	KERNELBASE.dll	~RtlInitUnicodeString (0x0012f2cc, "\Registry\Machine\System\CurrentControlSet\Services\Tcpip\Parameters")
20656	4:30:08.518 AM	1	KERNELBASE.dll	~NtOpenKey (0x0012f2fc, KEY_READ, 0x0012f2d4)
20657	4:30:08.518 AM	1	KERNELBASE.dll	~RtlInitUnicodeString (0x0012f2ec, "Hostname")
20658	4:30:08.518 AM	1	KERNELBASE.dll	~NtQueryValueKey (0x0000012c, 0x0012f2ec, KeyValueFullInformation, 0x0012f30c, 128, 0x0012f300)
20659	4:30:08.518 AM	1	KERNELBASE.dll	~memcpy (0x0012f404, 0x0012f330, 14)
20660	4:30:08.518 AM	1	KERNELBASE.dll	~NtClose (0x0000012c)
20661	4:30:08.518 AM	1	KERNELBASE.dll	~RtlInitUnicodeStringEx (0x0012f3c8, "IEBWIN7")
20662	4:30:08.518 AM	1	KERNELBASE.dll	~RtlUnicodeStringToAnsiString (0x0012f3d0, 0x0012f3c8, FALSE)
20663	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("IEBWIN7", "TEQUILABOOMBOOM")
20664	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("victim", "Wilbert")
20665	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("victim", "admin")
20666	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("victim", "admin")
20667	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("victim", "John Doe")
20668	4:30:08.518 AM	1	KERNELBASE.dll	IstrcmpA ("victim", "John")

## EMOTET KILLCHAIN

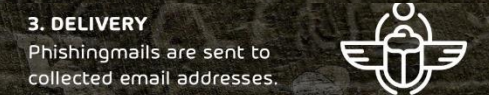
### 1. RECONNAISSANCE

Email addresses are collected with the help of an Emotet module.



### 2. WEAPONIZATION

An office file is distributed with a dangerous macro.



### 3. DELIVERY

Phishing mails are sent to collected email addresses.



### 4. EXPLOITATION

The user is prompted to execute the macro. The malware will be downloaded.

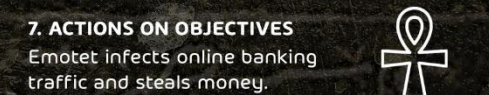
### 5. INSTALLATION

The malware embeds itself in the victim's system.



### 6. COMMAND AND CONTROL

C&C servers are contacted to load modules.



### 7. ACTIONS ON OBJECTIVES

Emotet infects online banking traffic and steals money.

# 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)

## EMOTET KILLCHAIN

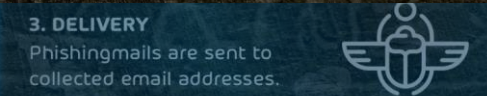
### 1. RECONNAISSANCE

Email addresses are collected with the help of an Emotet module.



### 2. WEAPONIZATION

An office file is distributed with a dangerous macro.



### 3. DELIVERY

Phishing mails are sent to collected email addresses.



### 4. EXPLOITATION

The user is prompted to execute the macro. The malware will be downloaded.

### 5. INSTALLATION

The malware embeds itself in the victim's system.



### 6. COMMAND AND CONTROL

C&C servers are contacted to load modules.

### 7. ACTIONS ON OBJECTIVES

Emotet infects online banking traffic and steals money.



# 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	dd147a5a3d54c1aaaef3a80b9fbda184
SHA1	4476fe9efa148677e33ee2f34ce82cf69dfe64fd
SHA256	9e40a7cc2a8d070dbcbb24fe37782ef70876f748bc9e8394d4391601ee4e6f57
SHA512	<a href="#">Show SHA512</a>
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 KILLCHAIN

- 1. RECONNAISSANCE**  
Email addresses are collected with the help of an Emotet module. 
- 2. WEAPONIZATION**  
An office file is distributed with a dangerous macro. 
- 3. DELIVERY**  
Phishing mails are sent to collected email addresses. 
- 4. EXPLOITATION**  
The user is prompted to execute the macro. The malware will be downloaded. 
- 5. INSTALLATION**  
The malware embeds itself in the victim's system. 
- 6. COMMAND AND CONTROL**  
C&C servers are contacted to load modules. 
- 7. ACTIONS ON OBJECTIVES**  
Emotet infects online banking traffic and steals money. 



# EMOTET KILL-CHAIN: EXPLOITATION



## EMOTET KILLCHAIN

### 1. RECONNAISSANCE

Email addresses are collected with the help of an Emotet module.



### 2. WEAPONIZATION

An office file is distributed with a dangerous macro.



### 3. DELIVERY

Phishing mails are sent to collected email addresses.



### 4. EXPLOITATION

The user is prompted to execute the macro. The malware will be downloaded.



### 5. INSTALLATION

The malware embeds itself in the victim's system.



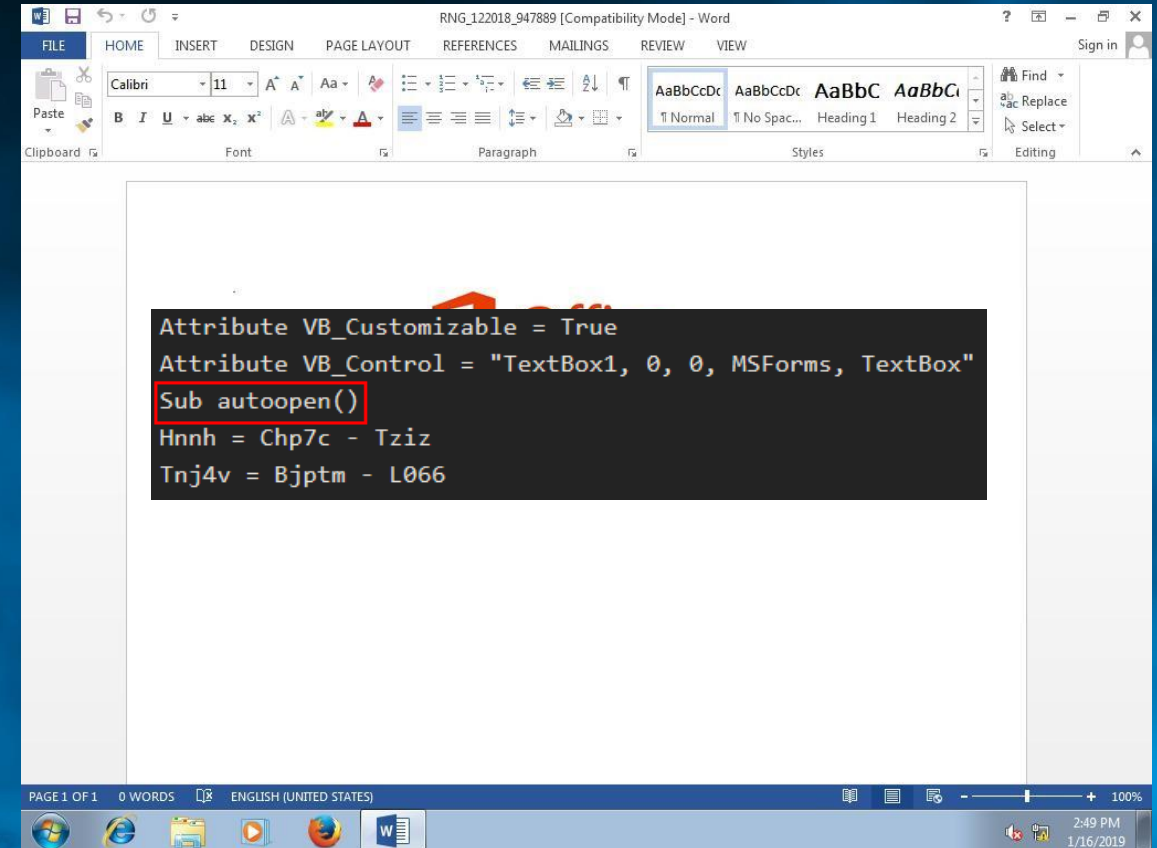
### 6. COMMAND AND CONTROL

C&C servers are contacted to load modules.



### 7. ACTIONS ON OBJECTIVES

Emotet infects online banking traffic and steals money.



# EMOTET KILL-CHAIN: INSTALLATION



HORNETSECURITY

## EMOTET KILLCHAIN

- 1. RECONNAISSANCE**  
Email addresses are collected with the help of an Emotet module. 
- 2. WEAPONIZATION**  
An office file is distributed with a dangerous macro. 
- 3. DELIVERY**  
Phishing mails are sent to collected email addresses. 
- 4. EXPLOITATION**  
The user is prompted to execute the macro. The malware will be downloaded. 
- 5. INSTALLATION**  
The malware embeds itself in the victim's system. 
- 6. COMMAND AND CONTROL**  
C&C servers are contacted to load modules. 
- 7. ACTIONS ON OBJECTIVES**  
Emotet infects online banking traffic and steals money. 

- ▶ 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

Process Name	PID	PPID	Working Set	Private Bytes	Working Set	Private Bytes	Process Name
infoagent.exe	1576	0.03	4.75 MB	IE8Win7\IEUser	Web DAV Client DLL		

# EMOTET KILL-CHAIN: C&C



HORNETSECURITY



➤ 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!

## EMOTET KILLCHAIN

- 1. RECONNAISSANCE**  
 Email addresses are collected with the help of an Emotet module.
 
- 2. WEAPONIZATION**  
 An office file is distributed with a dangerous macro.
 
- 3. DELIVERY**  
 Phishing mails are sent to collected email addresses.
 
- 4. EXPLOITATION**  
 The user is prompted to execute the macro. The malware will be downloaded.
 
- 5. INSTALLATION**  
 The malware embeds itself in the victim's system.
 
- 6. COMMAND AND CONTROL**  
 C&C servers are contacted to load modules.
 
- 7. ACTIONS ON OBJECTIVES**  
 Emotet infects online banking traffic and steals money.
 

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

UNIQUE\_ID\_DO\_NOT\_REMOVE - Editor

Daten Bearbeiten Format Ansicht Hilfe

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.

Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation

No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.

DO NOT RENAME OR MOVE the encrypted and readme files.

DO NOT DELETE readme files.

This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at

MelisaPeterman@protonmail.com

Or

MelisaPeterman@tutanota.com

BTC wallet:

14hVkm7Ft2rxDBFTNkRC3kGstMGp2A4hk

Ryuk

No system is safe

RyukReadMe - Editor

Daten Bearbeiten Format Ansicht Hilfe

Gentlemen!

Your business is at serious risk.

There is a significant hole in the security system of your company.

We've easily penetrated your network.

You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.

They can damage all your important data just for fun.

Now your files are crypted with the strongest military algorithms RSA4096 and AES-256.

No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.

Zusammenfassung		Transaktionen	
Adresse	14hVKm7Ft2rxDBFTNkRC3kGstMGp2A4hk	Anzahl der Transaktionen	4
Hash 160	2890a8b7bf8e92e5f024fd6cd260e7621c12b981	Insgesamt erhalten	10 BTC
		Endgültige Bilanz	0 BTC

P.S. Remember, we are not scammers.

We don't need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.

Just send a request immediately after infection.

All data will be restored absolutely.

Your warranty - decrypted samples.

contact emails

eliasmarco@tutanota.com

or

CamdenScott@protonmail.com

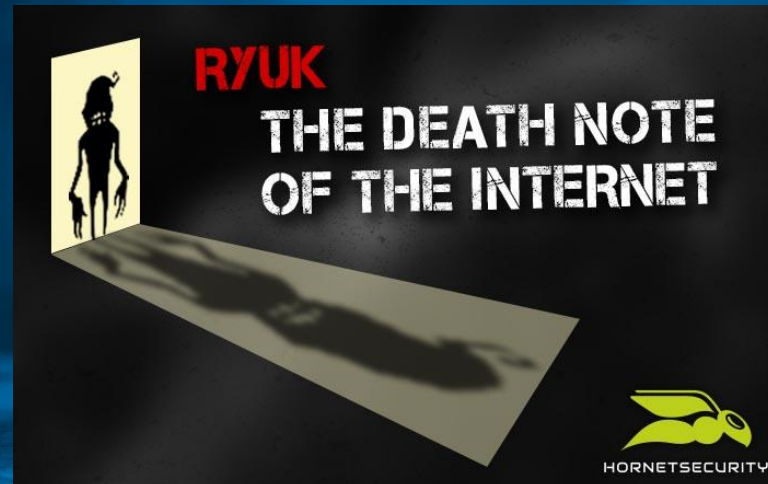


# FAZIT



HORNETSECURITY

- › 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



HORNETSECURITY

## CONTACT INFORMATION

Email: [sales@hornetsecurity.com](mailto:sales@hornetsecurity.com)

Phone: +49 511 515 464-200

[www.hornetsecurity.com](http://www.hornetsecurity.com)