

Emotet: A Sophisticated and Persistent Malware for Stealing Information, its Attack and Prevention Strategies

Deepak Reddy A R¹, Dr. Chandra Mohan B²

¹ Student at Vellore Institute of Technology, India ²School of Computer Science and Engineering, Vellore Institute of Technology, India ***

Abstract - Many people use internet every day for different activities like browsing, sending emails, banking, social media, and downloading files and videos. EMOTET is an advanced type of virus that mainly focuses on financial systems and individuals to poach personal and financial information. It spreads by false emails to people and also by replicating on itself. It can download other types of malware that attack the system even more, and it can encrypt sensitive data, making it inaccessible to the user. The US-CERT has already warned people about this malware. According to a cybersecurity company called CrowdStrike, dealing with EMOTET can cost up to \$1 million per incident. EMOTET usually spreads through phishing emails, which can contain malicious links or attachments, like fake PDFs or Microsoft Word documents. It's crucial to be careful and not click on suspicious links or attachments to avoid falling victim to this malware. This study intends to investigate the effects of Emotet on organizations and people as well as to find efficient preventative measures for this infection. The results of this paper provide valuable insights for businesses and individuals looking to protect themselves against the threat of Emotet and other sophisticated malwares.

Key Words: Emotet, Spider, Malware, Phishing, Cyber Security, Prevention, Banking.

1.INTRODUCTION

Emotet, also known as Geodo, is a type of malware that first surfaced in early 2014 and poses a significant threat to computers and networks[13]. Since its discovery in June 2014, the Emotet malware has grown into a major threat distributor that distributes and drops additional banking Trojans like Trickbot and IceDiD. This offers malware-as-aservice. It is difficult to locate and eliminate because it has been around for a while and altered over time. The virus is known as MUMMY SPIDER by renowned cybersecurity firm CrowdStrike, and it frequently changes its payloads to avoid discovery. Its primary goal is to gain access to an infected device, collect data from the target, and download additional malware payloads to steal credentials. On the Windows operating system, Emotet replicates itself into fixed areas, making it challenging to fully remove. It's a risky malware that criminals might use to propagate banking Trojans and ransomware like Ryuk and Trickbot.[12] Security experts at G DATA found over 33,000 distinct Emotet versions in just the first half of 2019. Emotet Variant 1 is extremely

dangerous due to its modular capabilities, which allow it to carry out coordinated DDOS attacks and steal money straight from the victim's bank account. These modules consist of spam bot, banking, and distribution modules.

Its most recent examples contain modules that can steal a variety of data from the target, including email client credentials, contact lists, web browser credentials, and email contents. It can propagate through LAN using spam or through WAN using SMB vulnerabilities. Recent spam campaigns by Emotet have been very effective at infecting users by making the emails appear more legitimate by using previously stolen email conversations.[5]

It can increase rights, brute-force local network credentials, harvest contacts and recent emails from Outlook, and proxy C2 traffic from other infected devices. As it collaborates with other types of malware, it spreads rapidly once it has access to a network and exposes devices to a wide range of threats. Emotet samples have increased recently, with spam campaigns mainly focusing on users in Lithuania, Greece, and Japan.[9] The most recent Emotet campaign, which made a big impression in many nations around the globe, is the subject of this report. The report examines the attack vector, maps the infrastructure used at different points in the campaign, and analyses Emotet's malicious payloads to determine their potential effect using a carefully crafted dataset.



Fig-1: Detected Emotet samples on a daily basis.

Emotet is among the priciest malware, with remediation expenses of up to \$1 million per incident, according to US-CERT. According to Sophos charts, Emotet regularly outperformed malware like GandCrab, HawkEye, Ursnif, Formbook, and AZORult in terms of frequency of sighting.



Every day, new Emotet spam campaigns and binaries are released, and countless spam emails are sent daily to guarantee widespread infections. [8]

2. LITERATURE SURVEY

Malware like Emotet, which has been around for a while and is spread through junk emails, is common. Malicious software, links, or document files with macro capability are the main entry points for it into a device.[1] In order to attract into clicking on dangerous URLs, the malware employs alluring wording like "your invoice" or "payment details." [4]. The virus was initially distributed through malicious JS files, but as it has advanced, it also makes use of documents with macro capability. Businesses and individuals have a difficult time analysing the malware because it is hard to detect. Additionally polymorphic, it has the capacity to alter itself each time it is downloaded onto the computer, making it difficult for AVs to successfully and pro-actively detect it. Furthermore, this malware lacks any signals and obtains updates via C & C servers in a way akin to how a laptop's operating system updates itself. Financial Trojans are among the malware types that this malware facilitates the installation of. Malware can also reveal private information like identities, passwords, and email addresses that have been taken.[4].

It is well known for its behavior, which involves surfing contact groups for email ids in specific and sending itself to the most important contacts. Since the mails are from genuine sources, they don't appear to be spam, and recipients are more likely to obtain the files because they are from reliable sources. The likelihood of the malware getting to the financial servers is significant if a user uses it as "password." Through Eternal Blue flaws connected to WannaCry attacks, the malware distributes [8].

A Banking Credentials Malware called Emotet Avoiding suspicious emails, according to the Stealer Pekta & Acarman team, can also help to prevent the device from becoming infected with adware [6]. For users of the Emotet malware, prior article didn't offer any SSA. This article will examine the user awareness problem in depth and give readers a thorough understanding of the Emotet malware's security situation. The purpose of this paper is to examine how similar, despite having different and largely unidentified origins, this specific group of malware's behaviours[12].

To identify particular network congestion patterns, ML techniques are frequently employed. With a 99 percent discovery rate, SSH congestion is found using a ripper learner [6]. To prevent models that depend on skewed port numbers that are given at random, they remove port nos. from attribute set. Compared specific flow exporters using ML techniques to enhance botnet congestion classification. The method involves using a 2-layer perception classifier to detect randomised bot congestion, which is a common technique used by bots to evade detection. Additionally, the

approach involves employing transient diligence to differentiate between benign and harmful bot congestion.

The proposed work forms the basis for detecting and preventing the injection of the Emotet money-lending Trojan and malignant network congestion.

The behaviour-based ML categorization model can identify some instances of Emotet infection without examining the PPC or IP addresses of the program. Overall, the approach offers a robust and effective solution for detecting and preventing the Emotet money-lending Trojan and other forms of bot congestion.

3. METHODOLOGY

Emotet is a type of malware that is primarily spread through spam mails that contain malicious attachments or links to infected websites. Once Emotet infects a system, it can carry out a variety of attacks.

3.1. Attack Methodology

Emotet is a type of malware that is primarily spread through spam mails that contain malicious attachments or links to infected websites. Once Emotet infects a system, it can carry out a variety of attacks. Here is a stepwise elaboration of Emotet's attack steps and methods:

- 1. An Emotet MS Word file is sent to the user as an email attachment.
- 2. The user accepts the license agreement when opening the Microsoft Word document, thereby allowing Emotet macros to run.
- 3. The macro runs encoded code inside the document using the terminal (cmd.exe) in the background.
- 4. Command Prompt launches to connect malicious Emotet sites.
- 5. The malicious sites drop payloads onto the target's machine.
- 6. It installs Trojan modules like Trickbot, IceDiD on target machine, allowing it to steal users' financial and confidential information.
- 7. C2C (command and control) connection is used by Emotet to send stolen information to attacker.



International Research Journal of Engineering and Technology (IRJET) www.irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072



Volume: 10 Issue: 04 | Apr 2023

Fig-2: Emotet's method of attack

Initial infection: Emotet infects a system through a spam email that contains a malicious attachment or a link to an infected website. The email is usually designed to look legitimate and convincing, encouraging the user to click on link or open the attachment.

AutoSeve 💽 🔡	2 10 14	errotet - Read-Only - Compatibility Mode - Saved to this PC	
File Home Insert	Design Layout References Mailings Collos - 11 + A' A' As B I U + ab X, X' A + A	Review View Heip Ø Sanch Ap Ξ : Ξ : Ξ : Ξ : Ξ : Ξ : Ξ : Ξ : Ξ : Ξ :	ABB ANBECCO ANBECCOF ANBECCOF ANBECCOF The Soldte Soldte Em. Emphase Interne E.
SECURITY WARNING Some	active content has been disabled. Click for more detail	Ende Content	
		terment Accept the license agreement These or which the details and the details the details of the details and the details	
		To accept and start Rhod cick Evable Editing and disk Evable Content	I

	Upgrade your edition of Microsoft Office
	Upgrade your edition of Microsoft Word
Microsoft Office Activation Witard	-
Microsoft Office	Upgrading your edition will add new features to Microsoft Word.
Activation Witard	Please, click Enable Editing and then click Enable Content.
Therkyou, Your copy of Microsoft Office is activated. To make you changes take effect click Enable Editing and Enable Context.	
	1) Office365
Microsoft Word	
	Operation did not consists surreset-lik bensus the fits was restart on IOS device
If you are opening the attached file with filicrosoft Word and you see a Protected view warning, then no values will be displayed until edding is enabled.	To view and edit document click Enable Editing and then click Enable Content.
	₩Microsoft Office 365
G Office 365	
This document only available for desktop or laptop versions of Microsoft Office Word.	You are attempting to open a file that was created in an earlier version
To open the document, follow these steps:	of Microsoft Office.
Click Enable editing button from the yellow bar above. Once you have enabled editing, please click Enable content button.	If the file opens in Protected View, click Enable Edition and then click Enable Content.
Microsoft Office Wizard	1 offer
Microsoft Office	Опісе
Transformation Wizard	* Disase analyse context to can the document
Downstion did not complete successfully because the file was created on Android device.	- Presser Enable Commit to See Sto Sociations
To view and edit document click "Enable Editing" and then click "Enable Content".	"If the file opens in Protected View, cick Enable Editing, and then cick Enable Content
	* You are attempting to open a life that was created in an earlier version of Microsoft Office.

Fig-3: Macros embedded in Word Document with potential Emotet.

Malware installation: Once Emotet is downloaded onto a system, it starts to install itself and establish persistence by modifying the registry and creating new services or tasks. This makes it difficult for antivirus software to detect and remove malware.

👶 Refresh	🛛 🍪 Opti	ons		>>> Sear	rch Proc	esses (Ctrl+K)		۶
Processes	Services	Network	Disk	1				
Name				PID	CPU	I/O total	Pri	*
	mscors	w.exe		2800				
	sppsvc.	exe		2964				
	svchost	.exe		3008	0.03		5	
6	taskhos	t.exe		3540				
	Isass.exe			504	0.15			
	Ism.exe			512				
🛍 wir	nlogon.exe			428				
4 🥽 exp	olorer.exe			272	0.57		3	
0	Telegram.	exe		2304	0.23		17	
- 0	chrome.ex	e		2856	0.83	2.27 kB/s		
	Chrome	exe		2636				
	Chrome	exe		2312			1	
	Chrome	exe		2020				
	chrome	exe		884			1	
	Chrome	exe		3980			5	
	Wireshark.	exe		3136	7.98	294 B/s	52	-
	dumpci	ap.exe		3876	0.07	250 B/s		1
195	ProcessHa	cker.exe		1772	2.13			
-4	b1f76c4b7	5fb1dc78b	o0f8	4804	77.88			
we we	rmgr.exe			2124	0.03		8	
								-

CPU Usage: 100.00% Physical memory: 1.34 GB (67.25%) Processes: 51

Fig-4: Malware infestation with Emotet



Network propagation: Emotet is designed to spread itself to other systems on the same network by using a variety of techniques such as brute-forcing passwords, exploiting vulnerabilities, and using stolen credentials. This allows Emotet to quickly infect multiple systems within an organization, making it more difficult to contain.

File	Edit	View G	0	Ca	ptu	e	A	naly	ze	St	atist	ics	Te	elept	nor	iy	Wi	reles	15	Too	Is	He	lp			
ii.	• 2	•	-	×	C		9	-	-		-	T	1				0	Q			ŧ.					
	Apply a d	splay filter .	. <	Ctrl	/>				_	_	_									C		-) 6	xpress	on		+
No,	т	ime		Sou	rce				_			De	stina	tion					1	Prote	lacel	L	ength	Inf	ю	k
	220 5	93.58688	2	21	5.5	3.2	14	.13	2			10	.0.	2.1	5					TCP			68	44	3 -	
	221 5	93.68180	7	21	5.5	3.2	14	.13	2			10	.e.	2.1	5					TLS	v1.:	2	1514	Se	rve	ł.
	222 5	93.68180		21	5.5	3.2	14	.13	2			10	.0.	2.1	5					TLS	v1.:	2	1233	Ap	pli	L.
	223 5	93.68181	1	21	5.5	3.2	14	.13	2			10	.0.	2.1	5					TCP			68	44	3 -	ł
	224 5	93.68187	з	10	0	2.1	5					21	6.5	8.2	14.	.13	2			TCP			54	49	17	ł
	225 5	93.91326	8	10	0.1	2.1	5					91	.10	8.5	6.1	150	8		10	SSL	-		451	Co	nti	i.
	226 5	93.91429		91	10	3.5	6.	150				10	.0.	2.1	5					TCP			68	44	3 -	ł
	227 5	93.91498	3	10	.0.	2.1	5					91	.10	8.5	6.1	150				TCP			54	49	166	ł.
	228 5	93.91604	1	91	10	3.5	6.	150				10	.0.	2.1	5					TCP			60	44	3 -	ł
	229 5	93.98349	2	10	0.	2.1	5					8.	8.4	.4						TCP			54	49	176	i
	230 5	93.98454	9	8.1	5.4	.4						10	.0.	2.1	5					TCP			60	44	3 -	ł
	231 5	94.04696	5	8.1	5.4	.4						10	.0.	2.1	5					TCP			60	44	3 -	ł
	232 5	94.04701	\$	10	0.1	2.1	5					8.	8.4	.4						TCP			54	49	176	ŝ.
	233 5	94.12935	5	91	10	3.5	6.	150				18	.0.	2.1	5					TCP			68	44	3 -	ł
	234 5	94.12940	3	10	0.1	2.1	5					91	.10	8.5	6.1	150				TCP			54	49	166	5
	235 5	94.32383	7	10	0.	2.1	5					14	9.1	54.	167	7.92	2			SSL			415	Co	nti	i.
	236 5	94.32547	3	14	.1	54.	16	7.9	2			10	.0.	2.1	5					TCP			68	44	3 -	ł
e (111																					*	
0 5	rame 1	1: 157 by	te	s o	n w	ire	. (125	6 b	bit	5),	1	000	0 3	33	33	00	01	00	02	08	00	27	c3	8a	1
DE	therne	t II, Sr	c:	Pc	sCo	mpu	1 0	3:8	a:7	7c	(08		001	8 4	90	00	00	67	11	01	fe	80	00	66	60	
> 1	Interne	t Protoc	01	Ve	rsi	on	6,	Sr	·c:	fe	:08:		002	8 1	fe	75	2f	df	d4	09	ff	02	00	99	60	
2	Jser Da	stagram P	ro	toc	01,	Si	c	Por	t:	54	16,	d I	603	8 4	90	00	00	01	00	02	82	22	02	23	60	
> 0	HCPv6											13		0	1d	90	90	ba	00	02	20	90	50	11	00	
												112		e 1	80	27	00	00	00	00	00	00	00	00	00	
													887		57	49	40	24	36	ad	46	40	40	33	4h	

Fig-5: Network Propagation of Emotet

Information stealing: Emotet is primarily designed to steal sensitive information from infected systems. It uses keylogging and web injection techniques to capture and exfiltrate data such as email credentials, banking information, and other personal information. Emotet can also steal information by intercepting network traffic and searching for sensitive data.

🚱 🔍 🛛 📕 🕨 ruveyd	a → AppData → Local → avatarearcon			✓ 4 Search ava P
Organize 👻 Include	in library 🔻 Share with 🔻 New folder			#• 🖬 0
🚖 Favorites	Name	Date modified	Туре	Size
📃 Desktop 🚺 Downloads	4 avatarearcon	11/26/2020 9:12 AM	Application	134 KB

Fig-6: Directory that Emotet cloned into.

Delivery of other malware: Once Emotet has established a foothold on a system, it can be used to deliver other types of malware such as ransomware or banking Trojans. Emotet can also be used to distribute spam emails and phishing attacks, allowing attackers to spread their reach and target more victims.



Fig-7: Files created and multiplied by Emotet.

<u>Command</u> and <u>control</u> <u>communication</u>: Emotet communicates with remote command-and-control servers to receive commands and update itself with new capabilities. This allows attackers to control the malware and carry out further attacks as needed.

svchost.e	xe (2776) (0)	2af0	000 -	- 0x3	000	00)									
00000640	72	a8	64	e8	0a	40	9c	c5	f4	71	ae	7b	7b	6a	07	ea	r.d@q.{{j
00000650	90	14	4f	8d	89	af	94	ab	b2	06	d4	02	6a	7b	98	1f	0j{
00000660	59	b9	3a	cd	54	fa	20	df	b2	2a	0a	e9	b8	dd	69	90	Y.:.T*i.
00000670	cO	29	d3	4e	d0	97	ed	66	CC	c5	19	49	06	7f	fa	5e	.).Nf1^
00000680	2c	7c	7b	85	1b	32	42	df	7b	95	25	02	03	01	00	01	, {2B. {.\$
00000690	a3	82	01	78	30	82	01	74	30	12	06	03	55	1d	13	01	x0t0U
00006a0	01	ff	04	80	30	06	01	01	ff	02	01	00	30	5c	06	03	00\
000006b0	55	1d	20	04	55	30	53	30	48	06	09	2b	06	01	04	01	UUOSOH+
00006c0	b1	3e	01	00	30	3b	30	39	06	80	2b	06	01	05	05	07	.>0;09+
000006d0	02	01	16	2d	68												http://cyber
000006e0	74																trust.omnircot.c
000006f0	85																om/repository.cf
0000700	6d.	30	07	06	05	60	83	4a	01	01	30	0e	06	03	55	1d	
0000710	Of	01	01	ff	04	04	03	02	01	e6	30	81	89	06	03	55	υ
00000720	1d	23	04	81	81	30	7f	a1	79	a4	77	30	75	31	0b	30	.#0y.w0u1.0
0000730	09	06	03	55	04	06	13	02	55	53	31	18	30	16	06	03	UUS1.0
00000740	55	04	0a	13	Of	47	54	45	20	43	6f	72	70	6f	72	61	UGTE Corpora
0000750	74	69	6f	6e	31	27	30	25	06	03	55	04	0b	13	1e	47	tion1'0%UG
00000760	54	45	20	43	79	62	65	72	54	72	75	73	74	20	53	6f	TE CyberTrust So
0000770	6c	75	74	69	6f	6e	73	2c	20	49	6e	63	2e	31	23	30	lutions, Inc.1#0
0000780	21	06	03	55	04	03	13	1a	47	54	45	20	43	79	62	65	!UGTE Cybe
0000790	72	54	72	75	73	74	20	47	6c	6f	62	61	6c	20	52	6f	rTrust Global Ro
000007a0	6f	74	82	02	01	a5	30	45	06	03	55	1d	1f	04	3e	30	ot0E>0
000007b0	3c	30	3a	a0	38	a0	36	86	34	68	74	74	70	3a	2f	2f	<0:.8.6.4http://
000007c0	77	77	77	2e	70	75	62	6c	69	63	2d	74	72	75	73	74	www.public-trust
000007d0	2e	63	6f	6d	2f	63	67	69	2d	62	69	6e	2f	43	52	4c	.com/cgi-bin/CRL
000007e0	2f	32	30	31	38	2f	63	64	70	2e	63	72	6c	30	1d	06	/2018/cdp.cr10
0000740	00		14	0-	0.4	10	04	1 4		10	00	40	10	17		10	n N
Re-read		-	Writ	e		Go	to.		16	5 byt	es p	er ro	w		•		Sav Network

Fig-8: Emotet has been executed and ASCII Codes appear here.

Evasion techniques: Emotet is designed to evade detection and avoid removal by using a variety of techniques such as obfuscation, anti-analysis techniques, and code injection.

In conclusion, Emotet is a highly advanced and persistent piece of malware that employs a variety of techniques to infiltrate computer systems, steal information, and propagate to other devices. It poses a serious danger to computer systems and networks due to its capacity for continuous evolution and collaboration with other malware.

3.2. Prevention Strategies

The malware known as Emotet is very cunning and changes all the time to attempt to evade the measures taken to stop it. As a result, there isn't a single method to stop it from contaminating your computer or your company. Instead, you need to attempt to stop it in a variety of ways.

For instance, you can instruct users on how to spot suspicious emails, use virus-checking software, frequently update computer programs, use filters to block spam emails, restrict what users can do on their computers, regularly make backup copies of crucial files, and require users to log in with two different methods. All of these measures can lessen the likelihood that Emotet will infect your company, but since Emotet is constantly evolving, you must continue to update and review them.



Fig-9: Emotet detection flow

To stop the spread of Emotet infection:

- Identify the infected system using Indicators of Compromise (IOCs) and isolate it.
- Identify the persistence of Emotet in Services, Scheduled Tasks, and Registry entries.
- Block Server Message Block communications between infected and other computers in the network.

- Reframe it and reset Local and domain credentials, change passwords for apps, and review and remove Emotet Phish emails from the Mail inbox.
- Implement and modify email filter and block policies, and stay away from using the Local Administrator and Domain Administrator accounts to access the compromised system.
- Transfer the infected system to a different VLAN to eliminate all artifacts while repairing the system.
- Educate employees on SSAs regarding Social Engineering and Phishing attacks.
- Warn staff members not to follow phishing links or open phishing attachments and not to share personal information, passwords, and usernames.
- Use GPO setup on Windows firewall rules to prevent client systems from sending inbound SMB communications.
- Implement a firewall and email policies to block, detect, and prevent malicious IP addresses and suspicious emails.
- Implement a least privilege policy that limits the amount of access that employees need to complete a particular task.
- Use DMARC to improve validation and lessen spam emails.
- Use designated administrators to restrict the no. of employees who have access to admin details.
- Establish two-factor authentication (2FA) for systems and apps to prevent unauthorized access.



Fig-10: Emotet prevention best practices



4. RESULTS

In order to penetrate computer systems, the Emotet malware uses social engineering strategies like spear phishing links and attachments. A phishing email that appears to be from a reliable source but may have been compromised is what begins the infection process. Emotet dropper is unknowingly downloaded once the recipient taps on the malicious link or opens the attachment. The Emotet executable is launched by the dropper's malicious macro, enabling it to create a C2C link and extract data. Using this method, spam emails can be sent from compromised accounts and distant email service providers.



Fig-11: Email Subjects of Emotet.



Fig-12: Emotet's Indicators of Compromise.

According to data research, Emotet malware is unfamiliar to most consumers. The job of identifying and preventing Emotet malware infections falls to organizations, but due to the malware's numerous variants, this can be difficult. It can be challenging to stop users from clicking on phishing links and files even with cybersecurity training. Implementing host-based intrusion protection systems and group policy settings that limit server message protocol (SMB) communications in a network are crucial for thwarting Emotet malware. SMB is a protocol that facilitates contact between devices and networks, but if Emotet is successful in breaching the SMB, it has the ability to infect entire domains, including clients and servers.





To sum up, more study is required to create practical strategies for lowering the risk posed by Emotet malware and protecting devices from it.

5. CONCLUSIONS

Due to its numerous variations and difficulty in detection, the Emotet virus is posing issues for numerous users and businesses. It becomes more difficult for people to get clear of it with each new version. The malware distributes to a person's devices the moment they click on a link or open an attachment. People, organisations should avoid opening suspicious emails, and staff members should be instructed not to rely on phishing links or documents in order to stop Emotet from infecting devices. In addition to outlining the value of Security Situational Awareness (SSA), the document provides tips on preventing Emotet infections. One important piece of advice is to keep an eye out for Emotet infections during SMB communications between client systems and to limit these communications by configuring Host-IPS or using group policy. This document offers advice on how to protect yourself from the Emotet malware in general.

REFERENCES

[1]. Niu, W., Li, T., Zhang, X., Hu, T., Jiang, T., & Wu, H. (2019). Using XGBoost to Discover Infected Hosts Based on HTTP Traffic. *Security and Communication Networks*, 2019.

[2]. Ceschin, F., Botacin, M., Gomes, H. M., Oliveira, L. S., &Grégio, A. (2019, November). Shallow security: On the

e-ISSN: 2395-0056 p-ISSN: 2395-0072

creation of adversarial variants to evade machine learningbased malware detectors. In Proceedings of the 3rd Reversing and Offensive-oriented Trends Symposium (pp. 1-9).

[3]. Bhardwaj, A., & Goundar, S. (2019). A framework for effective threat hunting. Network Security, 2019(6), 15-19. doi:10.1016/s1353 4858(19)30074-1.

[4]. Azab, A., Layton, R., Alazab, M., & Oliver, J. (2014). Mining malware to detect variants. 2014 Fifth Cybercrime and Trustworthy Computing Conference. doi:10.1109/ctc.2014.11.

[5]. Threat Advisory. (2019). The evolution of Emotet: From banking Trojan to threat distributor. https://www.symantec.com/blogs/threatintelligence/evolution-emotet-trojan-distributor.

[6]. Pektaş, A., & Acarman, T. (2018). Malware classification based on API calls and behavior analysis. IET Information Security, 12(2), 107-117. doi:10.1049/iet-ifs.2017.0430.

[7]. Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Applied Computer Systems, *24*(1), 9-17. [8]. Alert (TA18-201A) Emotet Malware. (July 20, 2018). Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-201A.

[9]. Emotet: Nastier Than WannaCry and Harder to Stop. (Feb 2010). A Sophos Whitepaper Retrieved from https://i.crn.com/sites/default/files/ckfinderimages/userfil es/images/crn/custom/2019/Sophos_LC_Q219_emotet nastier-than-wannacry-wp.PDF.

[10]. Littlefield (May 31, 2019). Three's a crowd: New Trickbot, Emotet & Ryuk Ransomware. Mediumhttps://littlefield.co/threes-a-crowd-new-trickbot-emotet-ryuk-ransomware-16d1e25f72f4.

[11]. Alexey Shulmin (Apr 9, 2015). The Banking Trojan Emotet: Detailed Analysis. Secure list. https://securelist.com/the-banking-trojan-Emotet-detailedanalysis/69560.

[12]. Cybereason Nocturnus (Apr 2, 2019). Triple Threat: Emotet Deploys Trickbot to Steal Data & Spread RYUK. Cybereason. https://www.cybereason.com/blog/triplethreat-emotet-deploys-trickbot-to-steal-data-spread-ryukransomware.

[13]. ESET Research (Nov 9, 2018). Emotet Launches Major new Spam Campaign. Welivesecurity. https://www.welivesecurity.com/2018/11/09/emotetlaunches-major-new-spam-campaign/

[14]. ASEC Report. Emotet Returns to Prey on Banking Information (2017).