blackhat EUROPE2023

DECEMBER 4-7 Excel London / UK



blackhat EUROPE2023

Breaching the Perimeter via Cloud Synchronized Browser Settings

Edward Prior

#BHEU @BlackHatEvents



ATTACKS

Cracking the perimeter

User Credentials







ATTACKS

Cracking the perimeter





AUTOMATION



Malware Phishing

Code Exec

Compromis e Cloud Infra

Code Exec

ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

Credential phishing



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

Credential phishing User interaction



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross–Site Request Forgery



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross–Site Request Forgery Context



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross–Site Request Forgery Context
- Browser Exploits



ATTACKS

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross–Site Request Forgery Context
- Browser Exploits Context



ATTACKS

Todays Goal

Demonstrate how cloud sync gives immense context to an attacker, and the tools to trigger remote payloads unavailable without sync.



INTRO

CASE STUDIES

ATTACKS

Whoami

- Edward Prior
- @JankhJankh
- Robotics -> Machine Learning -> Pentester/Red Teamer
- OSCP, OSCE, CRTE, ETC.
- 12 CVEs
- CTF Challenge Designer for AIV@DEF CON





INTRO

CASE STUDIES

ATTACKS

Outline

- Sync Introduction
- Case Studies
- Vuln Demos
- Prevention and Detection
- Automated Emulation





ATTACKS

Intro to Cloudsync

Cloudsync is a feature in every browser to allow for a consistent state between devices.



ATTACKS

Intro to Cloudsync

Cloudsync is a feature in every browser to allow for a consistent state between devices.

Features:

- Synced Settings, Extensions, Passwords, history, and user data
- Periodically pulls updates from a server



ATTACKS

Likelihood of compromise

- M365
- Google Business Suite
- Personal browser accounts





ATTACKS

Case Studies

All case studies assume a cloud synchronised account on a corporate device has been compromised, and that the browser is being used regularly.

Each case study was conducted against a fully patched Chrome, Edge, and Firefox browser.





ATTACKS

Case Study 1: Passive Actions





ATTACKS

Case Study 1: Passive Actions

1 save (0 reus	ed passwords sed, 0 weak)		Q Search	n passwords	Add password	
	Website ↓ F	Username	Password		Health ↑↓ ?	
	127.0.0.1:8080	admin	Secretpassword1	Ŕ		





ATTACKS

Case Study 1: Passive Actions

📃 Website 🦵	Username	Password	ł	-lealth ↑↓ ?	
127.0.0.1:8080	admin	Secretpassword1	<i>S</i>		
	"NON_UNIQUE_NAME":	"cardnumber 42424242424	242",		
	"ORIGINATOR_CACHE_G "ORIGINATOR_CLIENT_	UID": "", ITEM_ID": "",			
	"PARENT_ID": "",	OUE TAG", ""			
	"SPECIFICS": {	QUE_TAG : ,	15		
	"autofill": {	mben"			
	"usage_timestam	p": [
	"133408741800 1	00000"			
	"value": "42424	242424242"	2		
	}				





INTRO

ATTACKS

Case Study 1: Passive Actions

(0 reused, 0 weak)		Q Search	Q Search passwords Add password ····					
Website ↓	Username	Password		Health ↑↓ ?				
127.0.0.1:8080	admin	Secretpassword1	X		•••			
	<pre>"ORIGINATOR_CLIENT_ "PARENT_ID": "", "SERVER_DEFINED_UNIA "SPECIFICS": { "autofill": { "name": "cardnuarding"</pre>	ITEM_ID": "", QUE_TAG": "",						

<a class="c01216 card_clickable_title" href="https://jankhjankh.github.io/payment.html?firstname=Roy+B
unsen&email=Ro...en&cardnumber=424242424242424242424242428expmonth=09&expyear=2024&cvv=142&sameadr=on" title="TITL
E TO SECRET SITE" tabindex="-1" target="_self" dir="auto" rel="noreferrer">TITLE TO SECRET SITE





INTRO

ATTACKS

Case Study 1: Passive Actions

(0 reused, 0 weak)		Q Search	Q Search passwords Add password ····					
Website ↓	Username	Password		Health ↑↓ ?				
127.0.0.1:8080	admin	Secretpassword1	X		•••			
	<pre>"ORIGINATOR_CLIENT_ "PARENT_ID": "", "SERVER_DEFINED_UNIA "SPECIFICS": { "autofill": { "name": "cardnuarding"</pre>	ITEM_ID": "", QUE_TAG": "",						

DEFENCE

				an 117 i		
About Data Sync Node Brow	/ser Sear	rch Us	ser Events	Iraffic Log	Invalidations	
Refresh Last refresh time: 26/11/	72023, 9:18: Title	46 pm	Autofill			
Autoili	ID		null			
🕨 📙 Autofill Custom Data	Modific	ation Tin	ne null			
Autofill Profiles	Parent		r			
	Is Folde	r	true			
Bookmarks	Туре		Autofill			
Collection	External	ID	null			
Device Info	{	R": true,				
Edge E Drop	"NON_UNIQUE_NAME": "Autofill", "PARENT_ID": "r", "UNIQUE_SERVER_IAG": "Autofill"					
Edge Hub App Usage	"model }	Type": "A	lutofill"	, ,		
Edge Wallet						
Extension settings						
Extensions						
History Delete Directives						
😭 Nigori						
Passwords						
Preferences						
Send Tab To Self						
Sessions						
Typed URLs						
User Consents						

ATTACKS

Case Study 1: Passive Actions

Profiles / Passwords

Try the new management experience in Wallet

Offer to save passwords

Allow Microsoft Edge to save your passwords and help keep them secure

Automatically save passwords

Autofill passwords

Allow Microsoft Edge to automatically fill passwords.

More settings \checkmark

DEFENCE











ATTACKS

Case Study 2: Forced Navigation





ATTACKS

Case Study 2: Forced Navigation



DEFENCE

ATTACKS

Case Study 2: Forced Navigation



C	http	os://account.mici	x + rosoft.com/	?ref=setting	gs&refd=a	ccount.microsoft.com	
III Mici	rosoft account	Your info Roy B ⊠ roy.bunser	Privacy Sunse	Security	Reward	account.microsoft.com says account.microsoft.com:MC1=GUID=c8a3567d14224c7e97ce12e2622 93c5a&HASH=c8a3&LV=202 210&V=4&LU=1665894364313; MUID=0698EAC95A1E6F27313FF8165BE46E0D; _cs_c=0; _cs_id=1a38cd82-072b- a811-969b-14d2ac1a5558.1681619112.1.1681619112.1681619112.1 613561419.1715783112074; ClicktaleReplayLink=https:// dmz01.app.clicktale.com/Player.aspx?PID=1&UID=1&SID=1;	Î
	① Nev	er lose access to	your Micro	soft accoun	ıt	AMCV_EA76ADE95776D2EC7F000101%40AdobeOrg=15855401 35%7CMCIDTS%7C19464%7CMCMID%7C8605978461208358458303 5544961710443642%7CMCAAMLH-1 682223912%7C8%7CMCAAMB-1682223912%7C6G1ynYcLPuiQxYZrsz	
	M	icrosoft 365	OneDrive cl	aud starage	and more	OK	Ì

DEFENCE



ATTACKS

Case Study 3: File Directives





INTRO

CASE STUDIES

ATTACKS

Case Study 3: File Directives

(i) Problem loading page × +

C

ŵ

(i) file:////192.168.18.128/index.html

Access to the file was denied

The file at ///192.168.18.128/index.html is not readable.

• It may have been removed, moved, or file permissions may be preventing access.



23

SMB] NTLMv2-SSP Client : 192.168.18.129
SMB] NTLMv2-SSP Username : .\User
SMB] NTLMv2-SSP Hash : User::.:62ec61be6fd3f441:7F
8271E:010100000000000008067A3DAB3FBD90162BC599FA75E807A0
00510001001E00570049004E002D0054004400530054004D0037004
00570049004E002D0054004400530054004D0037004600410054004
002E004C004F00430041004C00030014004A004300470051002E004
004A004300470051002E004C004F00430041004C00070008008067F





INTRO

CASE STUDIES

ATTACKS

Case Study 3: File Directives

The support of the same of the same of the second	In material and a second second		이 이 눈에 들었는 것이 아니는 것이 아이들이 가 모두 말 못 같다.		
O Problem loading page	× +			Index of C:\U	sers\
\leftrightarrow \rightarrow C \bigcirc	ile:////192.168.18.	.128/index.html	☆	\leftrightarrow \rightarrow C	⑦ File
			I	ndex of	f C:\I
A Th	ccess to th e file at ///192. It may have bee	e file was denied 168.18.128/index.html is not read en removed, moved, or file permission	dable. ns may be preventing access.	Name All Users/ Default/ Default User Jankh/ 0365/	Size
			Try Again		
[SMB] NTLMv2-SSF [SMB] NTLMv2-SSF [SMB] NTLMv2-SSF 8271E:0101000000 00510001001E0057 00570049004E0020 002E004C004F0043	Client Usernar Hash 000000080 000490040 000540044 000410040	: 192.168.18.12 me : .\User : User::.:62ec6 067A3DAB3FBD901628 E002D0054004400536 400530054004D00376 C00030014004A00436	29 51be6fd3f441:7F 3C599FA75E807A0 0054004D0037004 004600410054004		

DEFENCE

AUTOMATION



Users\

Date Modified

5/7/22, 3:41:31 PM 4/16/23, 11:35:07 PM 5/7/22, 3:41:31 PM 12/2/23, 11:08:52 AM

CASE STUDIES INTRO ATTACKS Case Study 3: File Directives × + (i) Problem loading page Index of C:\Users\ (i) file:////192.168.18.128/index.html 3 ŵ • File C:/Users/ Index of C:\Users\ [parent directory] Size Access to the file was denied Name All Users/ Default/ The file at ///192.168.18.128/index.html is not readable. Default User/ Jankh/ It may have been removed, moved, or file permissions may be preventing access. Try Again prefs.js NTLMv2-SSP Client : 192.168.18.129 187 NTLMv2-SSP Username : .\User 188 NTLMv2-SSP Hash : User::.:62ec61be6fd3f441:7F 189 8271E:01010000000000008067A3DAB3FBD90162BC599FA75E807A0 <html> <script>function user_pref(data1, data2){ 00510001001E00570049004E002D0054004400530054004D0037004 console.log(data1) console.log(data2) 00570049004E002D0054004400530054004D0037004600410054004 }</script> 002E004C004F00430041004C00030014004A004300470051002E004 <script src="file:///</pre> 004A004300470051002E004C004F00430041004C00070008008067/

DEFENCE

AUTOMATION



Date Modified
5/7/22, 3:41:31 PM
4/16/23, 11:35:07 PM
5/7/22, 3:41:31 PM
12/2/23, 11:08:52 AM
10/12/23 4·30·39 AM

C:\Users\Jankh\AppData\Local\Mozilla\Firefox\Profiles\FirefoxSync\prefs.js - Sublime Text

File Edit Selection Find View Goto Tools Project Preferences Help

user_pref("services.sync.engine.prefs.modified", false); user_pref("services.sync.forms.lastSync", "1701480680.58"); user_pref("services.sync.forms.syncID", "vKek61Zw-H02");

C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\0khijcto.default-release\prefs.js"></script>



ATTACKS

Case Study 4: Protocol Handlers







ATTACKS

Case Study 4: Protocol Handlers



DEFENCE

A* 🖒				
<u> INo, thank</u>	KS			
×				
er and nersonal				
blisher above.				
Run Cancel				

ATTACKS

Case Study 5: Malicious Extensions

ATTACKS

Case Study 5: Malicious Extensions

id_rsa

×

+

i File C:/Users/User/.ssh/id_rsa

----BEGIN OPENSSH PRIVATE KEY----

പ

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAA/ NhAAAAAwEAAQAAAYEA9mZTUjLp/p0wV6Kt2fznAuQw7ny3F +uk2LkFsUh9hIo6Md9Q42F9ZM+MmVwJLXIP8ltTcoaMdGv0v Wg8irVrBUkb8xk/UJtwqi2RIPuOy3iU46EWzt3GaQgNzf7nl OqEf9C91DgFFetdmfJKkXEy64gKhdjz3a1ETNzU1EwSCMRb: LXiHJw3YpBoUnhXr0s3K9VYItHCOS289PuP16UL9QR5VCDh: ZRR1fcki76QIFXKPVLy/C6RjZmqIDp74i8KSIU2f80aGOrr) UbKcGRx6gpYd64NDJIAAUCtMZJ3hS6C88QIHNdoBz0VG6Xq /nDs3WFCaAu61ds19dngOKlrJb3DL2ndpYThk+2HAAAFkDzp EAAAGBAPZmU1Iy6f6dMFeirdn85wLkM058txesJWQZ4KHEyy YSKOjHfUONhfWTPjJlcCS1yD/JbU3KGjHRr9MArZDvWPXbz: /MZP1CbcKotkSD7jst4l00hFs7dxmkIDc3+5+2K3dhZfAc6 RXrXZnySpFxMuuICoXY892tREzc1NRMEgjEWyRUaN2RaMN7 FJ4V69LNyvVWCLRwjktvPT7j5elC/UEeVQg4SaOSgZU+QrE4 CBVyj1S8vwukY2ZqiA6e+IvCkiFNn/NGhjq619Gx60GSOV6: HeuDQySAAFArTGSd4UugvPECBzXaAc9FRu16o0NoPCd0M65c utXbNfXZ4DipayW9wy9p3aWE4ZPthwAAAAMBAAEAAAGBAMK(2N7t1kjUBpOyBd+PPxeSxiZMfrWEQkH0+7ILJeXlQDOHxTWc IK59voQ00yBSp5B4/02aLu+gbfQz8/ivZaLUKrG4ZW/KGhir

This page says

id_rsa:PGh0bWwgeG1sbnM9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkv eGh0bWwiPjxoZWFkPjxtZXRhI G5hbWU9ImNvbG9yLXNjaGVtZSIgY29udGVudD0ibGlnaHQgZGFyayI gLz48L2hIYWQ+PGJvZHk+PHByZ SBzdHlsZT0id29yZC13cmFwOiBicmVhay13b3JkOyB3aGl0ZS1zcGFjZTo gcHJlLXdyYXA7Ij4tLS0tL UJFR0IOIE9QRU5TU0ggUFJJVkFURSBLRVktLS0tLQpiM0JsYm5OemFD MXJaWGt0ZGpFQUFBQUFCRzV2Y m1VQUFBQUVibTI1WIFBQUFBQUFBQUFCQUFBQmx3QUFBQWR6YzJ ndGNuCk5oQUFBQUF3RUFBUUFBQVIFQ TltWIRVakxwL3Awd1Y2S3QyZnpuQXVRdzdueTNGNndsWkJuZ29jVExJ Z2NCRzBCdHFNclkKK3VrMkxrR

rpwZDdVcjJTtjO4n/zbr/yLjshctPXFvvSoRjKZHDK3xJAimjvsxp/Xb+mOxuzPW56PHHF NGc7TLvCtlg29zyWwjpCuiZpRYJzXDWmay8uXaTJz/Wkwn1Pm3zWn9SDaQTdkmrCYHVcqy Xojq8UZJxyOyNPAjxsuH4kF50npTAukUUW29CNU2RvSOAfj1/ttLdqFDl263es/QARiHRf NNe+JbUME+BuQywZZfRquuKq+Ho6Zj5xYSAyD2iOdFItOJ9VHCrUT1Yk18pAFnGaNXF96W JISwjzpHyexkcWdYkW9ywh8ji2qk7jpR1X21bTSk0hywBujCliOreVIfgqgOJGasQeMQAA

DEFENCE

Summary Of Case Studies

- Information Theft
- Full control of victim URLs
- Auth coercion
- Viewing local and remote files
- The ability to trigger external applications

ATTACKS

Attacks

ATTACKS

Forced Password Theft in Edge

DEFENCE

INTRO

CASE STUDIES

ATTACKS

Sensitive File Theft via Extensions

User starts browser

User is sent to C:/Users/User/.ssh /id_rsa Malicious Extension Reads the page and exfiltrates data

DEFENCE

AUTOMATION

User is redirected to their homepage.

ATTACKS

DEFENCE

ATTACKS

Sensiti

	A Carl								
V	e F	e	heft		om	Sha	are	Driv	/e
							turner and		
	\\192.168.18.128\d	lemoshare × -	-					-	>
	\leftarrow \rightarrow \uparrow	C ⊕→	Network > 192.168	3.18.128 > de	emoshare			Search demoshare	Q
	🕂 New - 🐰			V↓ Sort ~ 🔳	View ~				📑 Details
4	A Home	Name	^	Date mo	odified	Туре	Size		
	🔁 Gallery	C test.html		11/29/2	023 3:39 PM	Microsoft Edge HTM	1 KB		
>	📥 Roy - Personal								
C	6 🗖 🗋 te	st.html	× +						
	$\leftarrow \rightarrow C$	G i File	192.168.18.128/demos	share/test.html					
Т	est Share Drive Ex	tiltration							
	Elements	Console Sources	Network Performan	ce Memory	Application	Security Lighthou	ise CSS Ove	rview 프 🕂	
	→ Ø top ▼ ⑦	Filter	Default levels ▼ 🧧 7						
	accessibility.ty	peaheadfind.flashBar							
	app.installation.timestamp								
	133408090843795707								

DEFENCE

AUTOMATION

X

ATTACKS

Malware Dropping Via XSS

Chrome keeps you up to date

Chrome updates happen in the background automatically keeping you running smoothly and securely with the latest features.

DEFENCE

ATTACKS

Malware Dropping Via DOM Modification

DEFENCE

ATTACKS

RCE via Protocol Handler Vuln

DEFENCE

AUTOMATION

Open Windows Command Processor

ATTACKS

Leveraging Credentials and Context

DEFENCE

			<u>.</u>	0	×
☆ CD ¢	6	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	۲		-
ory ⑪	… ☆				Q
Search history			. Тробо	67	-
Recently closed Tabs from other devices		-	0 5	~	-
nt	ĺ				-
/manager	X_				
rday - Friday, Nov http://127.0.0.1:8080/man	ager/html				0
/manager	8:40 pm				0
Apache Tomcat/9.0.82	6:53 pm	-			
Apache Tomcat 9 Configuration Reference (. 6:50 pm				-
Microsoft account Home	6:42 pm				
https://account.microsoft.com/auth/comple.	6:42 pm				-
Microsoft account privacy notice	6:41 pm				+
https://account.microsoft.com/auth/comple.	6:41 pm				
Microsoft account Sign In or Create Your A.	6:36 pm				
					-

ATTACKS

Leveraging Credentials and Context

DEFENCE

ATTACKS

Desktop Credential Compromise

[SMB] NTLMv2-SSP Client : 192.168.18.129 NTLMv2-SSP Username : .\User NTLMv2-SSP Hash : User::.:62ec61be6fd3f441:7F 8271E:010100000000000008067A3DAB3FBD90162BC599FA75E807A0 00510001001E00570049004E002D0054004400530054004D0037004 00570049004E002D0054004400530054004D0037004600410054004 002E004C004F00430041004C00030014004A004300470051002E004 004A004300470051002E004C004F00430041004C00070008008067/

PS C:\Users\User\Desktop\hashcat-6.1.1> .\hashcat.exe -a 0 -m 5600 .\hash.txt .\rockyou.txt -w 3 -0 hashcat (v6.1.1) starting...

OpenCL API (OpenCL 2.1 AMD-APP (3516.0)) - Platform #1 [Advanced Micro Devices, Inc.] * Device #1: Ellesmere, 8128/8192 MB (6745 MB allocatable), 32MCU

Minimum password length supported by kernel: 0 Maximum password length supported by kernel: 27

Hashes: 1 digests; 1 unique digests, 1 unique salts Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates Rules: 1

Applicable optimizers applied: * Optimized-Kernel Zero-Byte Not-Iterated Single-Hash Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 626 MB

Dictionary cache hit: * Filename..: .\rockyou.txt Passwords.: 14345042 Bytes....: 139927340 Keyspace..: 14345042

USER::.:62ec61be6fd3f441:7fad17e80b2bb6146ede37a40548271e:01010000000000008067a3dab3fbd90162bc599fa 2d0054004400530054004d00370046004100540049004c0004003400570049004e002d0054004400530054004d003700460 00030014004a004300470051002e004c004f00430041004c00050014004a004300470051002e004c004f00430041004c000 0000010000000200000a74a588690d6960504aa1d55f090070980ea44ea46155bbe709a8c885673a3f60a001000000000

DEFENCE

ATTACKS

RCE via WinRM Request Forgery

HTTP Error 404. The requested resource is not found.

DEFENCE

Calcul	ator	_		×	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
∃ Star	ndard 🖫]		Ð	
				0	
				Ŭ	
AC N	IR M+	M-	MS	M~	
%	CE	С		\bigotimes	
1⁄x	<i>x</i> ²	$\sqrt[2]{x}$		÷	
7	8	9		×	
4	5	6		_	
1	2	3			
+/_	0			=	

ATTACKS

Lateral Movement

DEFENCE

AUTOMATION

Date modified

21/09/2022 11:25 AM 24/10/2023 9:49 PM 24/10/2023 9:24 PM 27/11/2023 9:47 PM

Туре

File folder File folder File folder File folder

ATTACKS

Summary of Attacks

- Information Theft
- Full control of victim URLs
- Auth coercion
- Viewing local and remote files
- The ability to trigger external applications
- Request Forgery attacks that circumvent SOP.
- Lateral movement

ATTACKS

Prevention

Disable setting sync on all browsers at a both a cloud and device level.

Harden browser settings via group policy.

Decouple your password manager from your browser.

Other recommendations:

- Investigate any other browsers in use in the organisation.
- Investigate if personal browser accounts are being used within the organisation.

DEFENCE

Detection

Alert on anomalous logins and actions within your external services. Periodically scan your enterprise for malicious extensions. Investigate anomalous browser subprocessess. Alert on excessive network activity (port scanning).

DEFENCE

INTRO

CASE STUDIES

ATTACKS

Automated Emulation

Automated emulation tool written in .NET.

Enables Sync In Browsers, and adds a malicious extension

Periodically Opens the Browser

https://github.com/JankhJankh/Syncy

DEFENCE

AUTOMATION

Malicious Extension Reads the sync config to inform attacks

Conducts malicious activity

Conclusion / Black Hat Europe Sound Bytes

Sync provides remote attackers with significant context into an enterprise environment, and some unique ways of leveraging that context to crack the perimeter.

Conclusion / Black Hat Europe Sound Bytes

Sync provides remote attackers with significant context into an enterprise environment, and some unique ways of leveraging that context to crack the perimeter.

Disable sync in enterprise environments.

Consider Syncy for your next attack simulation.

Questions?

Edward Prior at Aegis9 Socials: @JankhJankh

Syncy: https://github.com/JankhJankh/Syncy Whitepaper: Available on briefing page

