Supply Chain – The Major Target of Cyberespionage Groups

resecurity.com/blog/supply-chain-the-major-target-of-cyberespionage-groups

Mar 8, 2019
Cyberespionage

Resecurity has shared the acquired intelligence with law enforcement and partners for mitigation.

Friday, December 28, 2018 at 10:25 AM – Resecurity reached out to Citrix and shared an early warning notification about a targeted attack and data breach. Based on the timing and further dynamics, the attack was planned and organized specifically during Christmas period.

The incident has been identified as a part of a sophisticated cyberespionage campaign supported by nation-state due to strong targeting against government, military-industrial complex, energy companies, financial institutions and large enterprises involved in critical areas of economy.

Based our recent analysis, the threat actors leveraged a combination of tools, techniques and procedures (TTPs) allowing them to conduct a targeted network intrusion to access at least 6 terabytes of sensitive data stored in the Citrix enterprise network, including e-mail correspondence, files in network shares and other services used for project management and procurement.

We forecast a continued growth of targeted cyber-attacks on supply chains of government and large enterprises organized by state-actors and sophisticated cyberespionage groups.

Updated (4:49 PM Monday, March 11, 2019 PDT)

Below are the indicators of IRIDIUM activity available for disclosure (for today). We will update the list with new information once it becomes available.

We would like to thank the following organizations for their timely assistance and collaboration regarding the malicious network activity during the Winter 2018 period: DHL, NBC (National Bank of Canada), Skrill, PayPal and Canadian Centre for Cyber Security.

Source IPs:

178.131.21[].19[] (Iran)
5.115.23[].11[] (Iran)
5.52.14[].23[] (Iran)

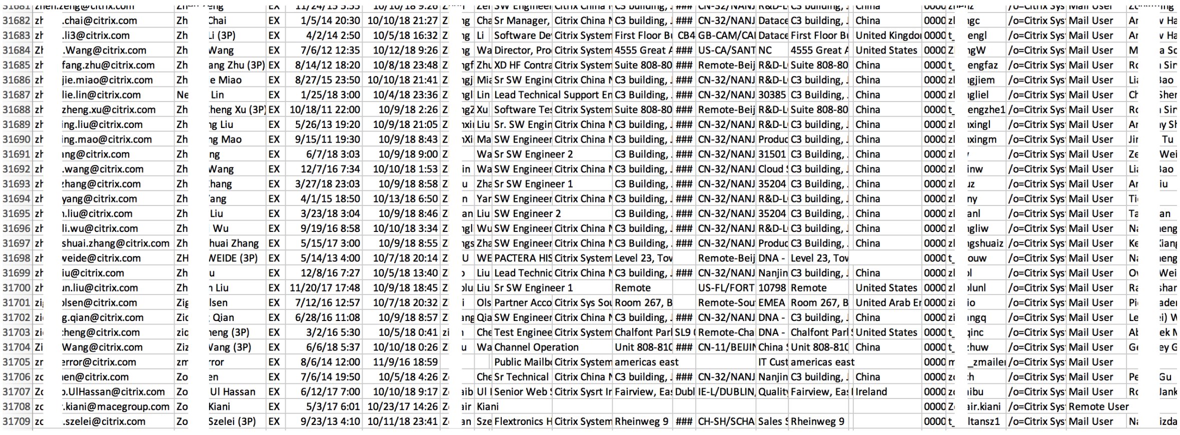
Used proxies:

23.237.104.90 – Canada (VPN)
194.59.251.12 – USA (VPN)
185.244.214.198 – Poland
138.201.142.113 – Germany
92.222.252.193 – France (Nov 29, 2018)
51.15.240.100 – France (Dec 7, 2018) x 3 times
185.220.70.135 – Germany (Dec 7, 2018) x 5 times

(The list will be updated)

Updated (5:09 PM Monday, March 11, 2019 PDT)

The Global Access List (GAL) acquired as the result of password-spraying (on Citrix employee accounts), which is a type of attack for brute-forcing and credential-stuffing, includes 31,738 records. The threat actors leveraged it for further reconnaissance and accounts compromise. Based on our analysis, one of these elevated actions was conducted on Monday, October 15, 2018 at 1:57 AM.



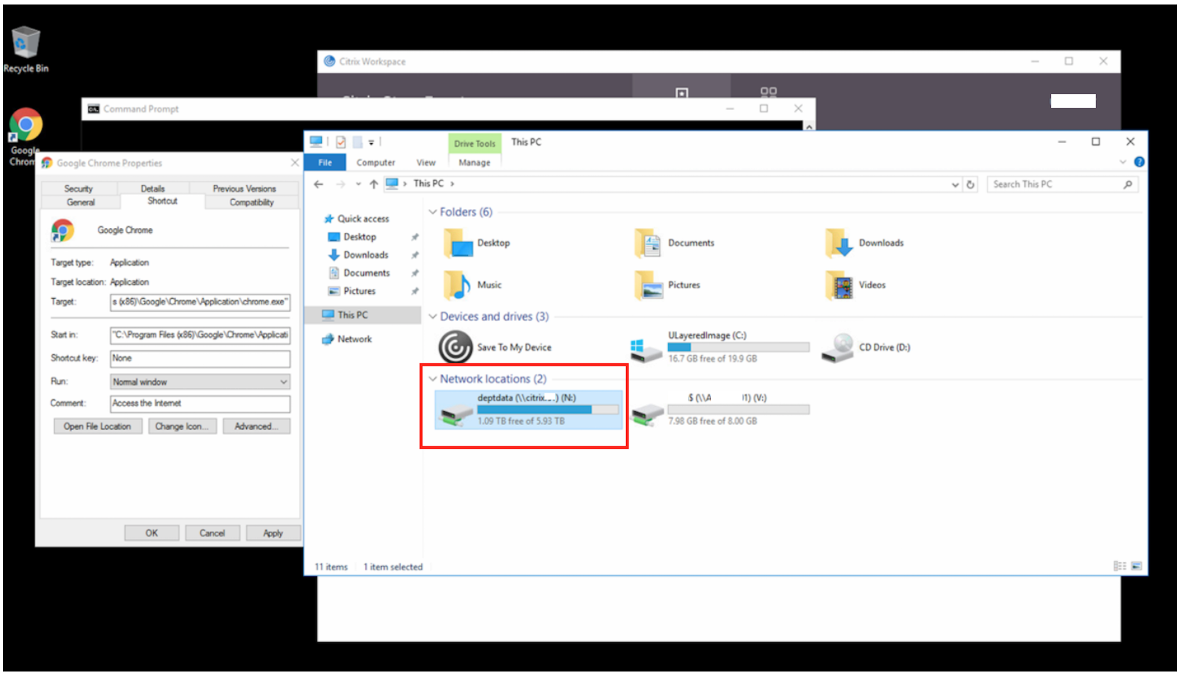
31681	zhen.zeng@citrix.com		Zh	eng	EX	11/24/15 3:55	10/10/18 9:26	Z		Zer	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	R&D-L	C3 building, J	China	0000	zh	z	/o=Citrix Sys	Mail User	Zc	ng
31682	zh	.chai@citrix.com	Zh	Chai	EX	1/5/14 20:30	10/10/18 21:27	Z	ng	Cha	Sr Manager,	Citrix China N	C3 building, J	###	CN-32/NANJ	Datace	C3 building, J	China	0000	zl	ngc	/o=Citrix Sys	Mail User	Ar	v Ha
31683	zh	.li3@citrix.com	Zh	Li (3P)	EX	4/2/14 2:50	10/5/18 16:32	Z	ng	Li	Software De	Citrix System	First Floor Bu	CB4	GB-CAM/CAI	Datace	First Floor Bu	United Kingdo	0000	t_	engl	/o=Citrix Sys	Mail User	Ar	v Ha
31684	Zh	.Wang@citrix.com	Zh	Wang	EX	7/6/12 12:35	10/12/18 9:26	Z	ng	Wa	Director, Pro	Citrix System	4555 Great A	###	US-CA/SANT	NC	4555 Great A	United States	0000	Z	ngW	/o=Citrix Sys	Mail User	M	a Sc
31685	zh	fang.zhu@citrix.com	Zh	ang Zhu (3P)	EX	8/14/12 18:20	10/8/18 23:48	Z	ngf	Zhu	XD HF Contra	Citrix System	Suite 808-80	###	Remote-Beij	R&D-L	Suite 808-80	China	0000	t_	engfaz	/o=Citrix Sys	Mail User	Ro	Sir
31686	zh	jie.miao@citrix.com	Zh	e Miao	EX	8/27/15 23:50	10/10/18 21:41	Z	ngj	Mia	Sr SW Engine	Citrix China N	C3 building, J	###	CN-32/NANJ	R&D-L	C3 building, J	China	0000	zl	ngjiem	/o=Citrix Sys	Mail User	Lia	Bao
31687	zh	lie.lin@citrix.com	Ne	Lin	EX	1/25/18 3:00	10/4/18 23:36	Z	ngl	Lin	Lead Technical Support En		C3 Building, .	###	CN-32/NANJ	30385	C3 Building, .	China	0000	zl	ngliel	/o=Citrix Sys	Mail User	Ch	Sher
31688	zh	zheng.xu@citrix.com	Zh	heng Xu (3P)	EX	10/18/11 22:00	10/9/18 2:26	Z	ngZ	Xu	Software Tes	Citrix System	Suite 808-80	###	Remote-Beij	R&D-L	Suite 808-80	China	0000	t_	engzhe1	/o=Citrix Sys	Mail User	Ro	Sir
31689	zh	ing.liu@citrix.com	Zh	g Liu	EX	5/26/13 19:20	10/9/18 21:05	Z	xin	Liu	Sr. SW Engin	Citrix China N	C3 building, J	###	CN-32/NANJ	R&D-L	C3 building, J	China	0000	zl	xingl	/o=Citrix Sys	Mail User	Ar	y Sh
31690	zh	ing.mao@citrix.com	Zh	g Mao	EX	9/15/11 19:30	10/9/18 8:43	Z	Xi	Ma	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	Produc	C3 building, J	China	0000	zl	xingm	/o=Citrix Sys	Mail User	Jin	Tu
31691	zh	ang@citrix.com	Zh	ng	EX	6/7/18 3:03	10/9/18 9:00	Z		Wa	Sr SW Engineer 2		C3 Building, .	###	CN-32/NANJ	31501	C3 Building, .	China	0000	zl	'	/o=Citrix Sys	Mail User	Ze	Wei
31692	zh	.wang@citrix.com	Zh	Wang	EX	12/7/16 7:34	10/10/18 1:53	Z	in	Wa	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	Cloud S	C3 building, J	China	0000	zl	inw	/o=Citrix Sys	Mail User	Lia	Bao
31693	zh	zhang@citrix.com	Zh	hang	EX	3/27/18 23:03	10/9/18 8:58	Z	u	Zha	Sr SW Engineer 1		C3 Building, .	###	CN-32/NANJ	35204	C3 Building, .	China	0000	zl	uz	/o=Citrix Sys	Mail User	Ar	iu
31694	zh	yang@citrix.com	Zh	Yang	EX	4/1/15 18:50	10/13/18 6:50	Z	n	Yar	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	R&D-L	C3 building, J	China	0000	zl	ny	/o=Citrix Sys	Mail User	Ti	
31695	zh	n.liu@citrix.com	Zh	Liu	EX	3/23/18 3:04	10/9/18 8:46	Z	an	Liu	SW Engineer 2		C3 Building, .	###	CN-32/NANJ	35204	C3 Building, .	China	0000	zl	anl	/o=Citrix Sys	Mail User	Ta	an
31696	zh	li.wu@citrix.com	Zh	Wu	EX	9/19/16 8:58	10/10/18 3:34	Z	ngl	Wu	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	R&D-L	C3 building, J	China	0000	zl	ngliw	/o=Citrix Sys	Mail User	Na	heng
31697	zh	shuai.zhang@citrix.com	Zh	huai Zhang	EX	5/15/17 3:00	10/9/18 8:55	Z	ngs	Zha	SW Engineer	Citrix China N	C3 Building, .	###	CN-32/NANJ	Produc	C3 Building, .	China	0000	zl	ngshuaiz	/o=Citrix Sys	Mail User	Ke	Xiang
31698	zh	weide@citrix.com	ZH	WEIDE (3P)	EX	5/14/13 4:00	10/7/18 20:14	Z	U	WE	PACTERA HIS	Citrix System	Level 23, Tov		Remote-Beij	DNA -	Level 23, Tov		0000	t_	ouw	/o=Citrix Sys	Mail User	Na	heng
31699	zh	iu@citrix.com	Zh	u	EX	12/8/16 7:27	10/5/18 13:40	Z	o	Liu	Lead Technic	Citrix China N	C3 building, J	###	CN-32/NANJ	Nanjin	C3 building, J	China	0000	zl	l	/o=Citrix Sys	Mail User	Ov	Wei
31700	zh	un.liu@citrix.com	Zh	n Liu	EX	11/20/17 17:48	10/9/18 18:45	Z	olu	Liu	Sr SW Engineer 1		Remote		US-FL/FORT	10798	Remote	United States	0000	zl	olunl	/o=Citrix Sys	Mail User	Ra	shar
31701	zi	olsen@citrix.com	Zig	lsen	EX	7/12/16 12:57	10/7/18 20:32	Z	i	Ols	Partner Acco	Citrix Sys Sou	Room 267, B		Remote-Sou	EMEA	Room 267, B	United Arab Er	0000	zi	io	/o=Citrix Sys	Mail User	Pi	ader
31702	zi	g.qian@citrix.com	Zic	Qian	EX	6/28/16 11:08	10/9/18 8:57	Z	ang	Qia	SW Engineer	Citrix China N	C3 building, J	###	CN-32/NANJ	DNA -	C3 building, J	China	0000	zi	ngq	/o=Citrix Sys	Mail User	Le	i) W
31703	zi	heng@citrix.com	zic	heng (3P)	EX	3/2/16 5:30	10/5/18 0:41	zi	n	Che	Test Enginee	Citrix System	Chalfont Parl	SL9 (	Remote-Cha	DNA -	Chalfont Parl	United States	0000	t_	qinc	/o=Citrix Sys	Mail User	Ab	ek M
31704	Zi	Wang@citrix.com	Ziz	Wang (3P)	EX	6/6/18 5:37	10/10/18 0:26	Z	u	Wa	Channel Operation		Unit 808-810	###	CN-11/BEIJIN	China S	Unit 808-810	China	0000	t_	zhuw	/o=Citrix Sys	Mail User	Ge	ey G
31705	zr	error@citrix.com	zm	rror	EX	8/6/14 12:00	11/9/16 18:59				Public Mailb	Citrix System	americas east			IT Cust	americas east		0000	m	_zmailer	/o=Citrix Sys	Mail User		
31706	zo	en@citrix.com	Zo	en	EX	7/6/14 19:50	10/5/18 4:26	Z		Che	Sr Technical	Citrix China N	C3 building, J	###	CN-32/NANJ	Nanjin	C3 building, J	China	0000	zo	h	/o=Citrix Sys	Mail User	Pe	Gu
31707	Zo	o.UlHassan@citrix.com	Zo	Ul Hassan	EX	6/12/17 7:00	10/10/18 9:17	Z	aib	Ul I	Senior Web S	Citrix Sysrt Ir	Fairview, Eas	Dubl	IE-L/DUBLIN,	Quality	Fairview, Eas	Ireland	0000	zo	aibu	/o=Citrix Sys	Mail User	Ro	Jank
31708	zo	.kiani@macegroup.com	Zo	Kiani	EX	5/3/17 6:01	10/23/17 14:26	Z	air	Kiani									0000	Z	air.kiani	/o=Citrix Sys	Remote User		
31709	zo	.szelei@citrix.com	Zo	Szelei (3P)	EX	9/23/13 4:10	10/11/18 23:41	Z	an	Sze	Flextronics H	Citrix System	Rheinweg 9	###	CH-SH/SCHA	Sales S	Rheinweg 9		0000	t_	ltansz1	/o=Citrix Sys	Mail User	Na	izda

Password-spraying was one of the most commonly used techniques by Mabna Institute hackers and their associates during the early stage of the attacks to gain a foothold in the victim's environment. More information about their techniques is available in FBI Flash Alert (ME-000092-TT):

- Leveraging the initial group of compromised accounts, download the Global Address List (GAL) from a target's email client, and perform a larger password spray against legitimate accounts.
- Using the compromised access, malicious actors attempt to expand laterally (e.g., via Remote Desktop Protocol or other means) within the network, and perform mass data exfiltration.

Updated (8:55 PM Monday, March 11, 2019 PDT)

As a result, threat actors conducted network intrusion to access data in Citrix infrastructure remotely.



Google Chrome

Target type: Application

Target location: Application

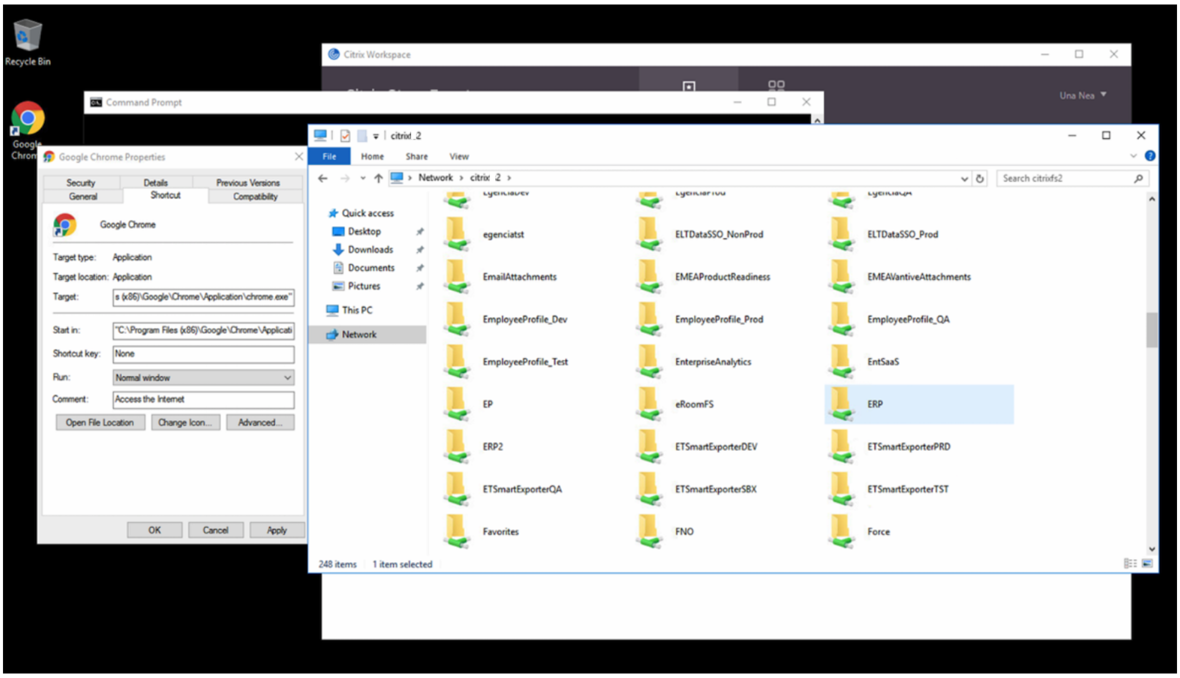
Target: s (x86)\Google\Chrome\Application\chrome.exe"

Start in: "C:\Program Files (x86)\Google\Chrome\Applicati

Shortcut key: None

Run: Normal window

Comment: Access the Internet



Google Chrome

Target type: Application

Target location: Application

Target: s (x86)\Google\Chrome\Application\chrome.exe"

Start in: "C:\Program Files (x86)\Google\Chrome\Applicati

Shortcut key: None

Run: Normal window

Comment: Access the Internet

Mitigation Measures:

– Azure AD and ADFS best practices: Defending against password spray attacks
https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/

– Spray you, spray me: defending against password spraying attacks
https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks