AEC

Aktivity Cobalt Group v ČR v říjnu 2019
Cobalt Group activities in Czech Republic in October 2019

5. prosince 2019 / December 5 2019

Shrnutí

Kriminální skupina Cobalt Group (také známá jako Cobalt Gang nebo Cobalt Spider) zahájila nejpozději 2. října 2019 phishingovou kampaň cílenou prokazatelně na velké množství finančních institucí v České republice. Cobalt Group je pokročilá skupina v oblasti kybernetického zločinu, která útoky na systémy ATM a SWIFT odcizila dle některých odhadů řádově 1 mld EUR.

AEC Cyber Defense Center zveřejňuje IOC (indikátory kompromitace) zanechané skupinou při této kampani k získání a udržení přístupu. Vzhledem k tomu, že mnoho z níže uvedených IOC nebylo dříve veřejně známo, doporučujeme bezpečnostním týmům, aby se ujistili, že nedošlo ke kompromitaci jejich prostředí.

Summary

Known threat group Cobalt Group (a.k.a. Cobalt Gang or Cobalt Spider) launched a phishing campaign no later than October 2, 2019 targeting large number of financial institutions in the Czech Republic. Cobalt Group is an advanced cyber-crime group known to have targetted primarily ATM systems and SWIFT and stealed 1 bln EUR.

AEC Cyber Defense Center publishes IOCs (Indicators of Compromise) left by the group during this campaign to gain and maintain access. As many of these IOCs were previously unknown, we advise the security teams to use them to confirm their environments were/are not compromised.

www.aec.cz/cdc
cdc@aec.cz

AEC

Indikátory kompromitace / Indicators of Compromise

Type	IOC	Note
Domain	adminassistance.info	
Domain	0345432456.info	
Domain	octetfruitsllc.com	
SMTP Sender	xxxxx.xxxxx@o2.cz	
SMTP Sender	xxxxx.xxxxx@o2.cz	
SMTP Subject	aplatby po splatnosti	
SMTP Subject	FW: aplatby po splatnosti	
IPv4	213.252.244.232	
IPv4	88.119.175.131	
IPv4	185.205.209.243	
IPv4	193.124.16.34	
IPv4	94.156.35.38	
IPv4	86.106.131.172	
IPv4	176.119.28.3	
IPv4	91.214.124.20	
IPv4	45.147.229.223	
IPv4	45.125.65.101	
IPv4	185.61.149.16	
MD5	7d339ee10e6561f1fb9de3ab05dd4fb8	admin32.exe
MD5	73e881fb0eab8aa8182e62a466e9577d	winsvc.exe
MD5	bc0787ef7585109165b4e4ef0e04d309	java.exe
MD5	c91fcdcbf8f4c671257677664ad34eef	Bbxlcmd.exe
MD5	7ecb1518c3fdf0d9e2c16cd46871cf01	memrun.exe
MD5	b304632428e197d749a228ef9959112c	ImageConvertor.ps1
MD5	ab39446562baad0cfe578c503a993026	svchosts.exe
SHA1	ffc2be94e5e6a28150cae7b092fc6fd8efafe4d1	admin32.exe
SHA1	7c5af2a594fbb65c4cd732d0cea53588035b186f	winsvc.exe
SHA1	9376ac7687b0165e6078362e07731957a48fbf6a	java.exe
SHA1	7e4f0728a70d8aef577536bf8a359c9053a7528d	svchosts.exe
SHA256	bc504b51563959abb11a456ef926b255d8dd679710cedcc1ed7815e8be4e877c	admin32.exe
SHA256	70a58b1cfbbde2b83ae1948f49631beb293997cb98a8966c88c55a8e62be694e	winsvc.exe
SHA256	ccee5a899a62b683fa1f0aaa806ac40c30c3d98e6a96f53b3d5d2fb7e0c886c0	java.exe
SHA256	c6c3bbb3dbbbd4ed4347868249276043404f308ad4f4f32265de04ee8b31a841	Bbxlcmd.exe
SHA256	b827be4e292ba7dc0c9d4e76168456ee9ea3b5bfd00aaae184ecc7d06bcd8f02	memrun.exe
SHA256	7f59a090e1c476fd4e4f715a3fc11cd1d0a4760fda79d689a793f91a1ca2ad7c	E0DB.tmp
SHA256	03ac2877e1a21ac79a1498032b5932a2107ae168d923c31ac501259027cc299f	svchosts.exe
SHA256	03ec7506586d4a469bbf7f3a3f50ade81a9fcac666c8c1363be62d7e3ff8d6e8	faktura.doc