Financial spear-phishing campaigns pushing RATs

cyjax.com/2021/05/27/financial-spear-phishing-campaigns-pushing-rats/

May 27, 2021

Blog

By William Thomas 27th May 2021

On 12 May, the FBI Cyber Division issued a TLP:WHITE Private Industry Notification. This concerned a spear-phishing campaign distributing messages that masqueraded as financial institutions to push fake Windows apps containing remote access Trojans (RATs). The most recent attack impersonated a US-based financial institution to target an American renewable energy company. The spear-phishing email referenced a fictitious loan and instructed the target organisation's employees to download a Windows application so as to complete the loan process to receive $62 million. [1]

The email appeared to have arrived from a UK-based financial institution and confirmed that the US firm's loan had been accessed and could be processed using the fake Windows application. The email contained two PDF files, one of which used the names and likeness of the UK's National Crime Agency (NCA) and the other appeared to contain SWIFT information. The email had a URL from which to download the application; it also contained the username and password to access it.

The threat actors had registered a domain (secureportal[.]online) through which they can share the links to the fake Windows applications. At least four firms were impersonated on this one domain: Cumberland Private UK, Truist, FNB America, and MayBank. [2, 3, 4]

Cyjax analysts investigated the indicators of compromise disclosed by the FBI and uncovered additional files and phishing pages connected to this ongoing campaign that has been running since at least 2017. The attackers have masqueraded as various financial institutions from around the world – not just from the US and UK – this includes organisations from Panama, West Africa, Malaysia, and China. They have posed as investment banks to deliver a similar backdoored Windows application that was described in the FBI PIN.

We analysed the hosting services and name servers used by the initial domain (secureportal[.]online) shared publicly by the FBI for patterns. This revealed multiple other sites using the same servers, created in the same time frame, masquerading as investment banks:

Creation Date	Domain	IP	Name Servers	Host

Creation Date	Domain	IP	Name Servers	Host
2017-05-03	thebnymellon[.]com	66.85.156.85	AS19318 IS-AS-0	AS20454 SECURED SERVERS
2017-06-27	bbtcorpo[.]com	66.85.156.85	AS19318 IS-AS-1	AS20454 SECURED SERVERS
2018-04-24	bceaoportal[.]com	108.170.31.123	AS19318 IS-AS-1	AS20454 SECURED SERVERS
2018-05-01	esecurebanking[.]online	108.170.31.123	AS19318 IS-AS-1	AS20454 SECURED SERVERS
2019-01-24	scotia-itrade[.]online	66.85.156.85	AS19318 IS-AS-1	AS20454 SECURED SERVERS
2019-03-19	secureportal[.]online	108.170.31.123	AS19318 IS-AS-2	AS20454 SECURED SERVERS
2019-05-31	scotia-itrade[.]com	66.85.156.85	AS19318 IS-AS-6	AS20454 SECURED SERVERS
2019-08-07	multibankpa[.]com	66.85.156.86	AS19318 IS-AS-6	AS20454 SECURED SERVERS
2020-02-21	securebankapp[.]com	66.85.156.85	AS19318 IS-AS-4	AS20454 SECURED SERVERS
2020-02-25	trfincorporation[.]online	108.170.61.187	AS19318 IS-AS-6	AS20454 SECURED SERVERS
2020-09-02	chasetrustus[.]com	108.170.52.156	AS19318 IS-AS-6	AS20454 SECURED SERVERS
2020-12-04	cponlineuk[.]com	192.119.92.32	AS19318 IS-AS-6	AS54290 HOSTWINDS
2020-12-07	securemailbox[.]online	66.85.156.86	AS19318 IS-AS-3	AS20454 SECURED SERVERS
2021-01-10	cpbkuk[.]com	192.119.92.32	AS19318 IS-AS-6	AS54290 HOSTWINDS
2021-03-26	psbcn[.]com	104.168.138.242	AS19318 IS-AS-6	AS54290 HOSTWINDS
2021-05-18	securebankapp[.]online	66.85.156.86	AS19318 IS-AS-6	AS20454 SECURED SERVERS

Fig. 1 – Campaign infrastructure connected to this campaign.

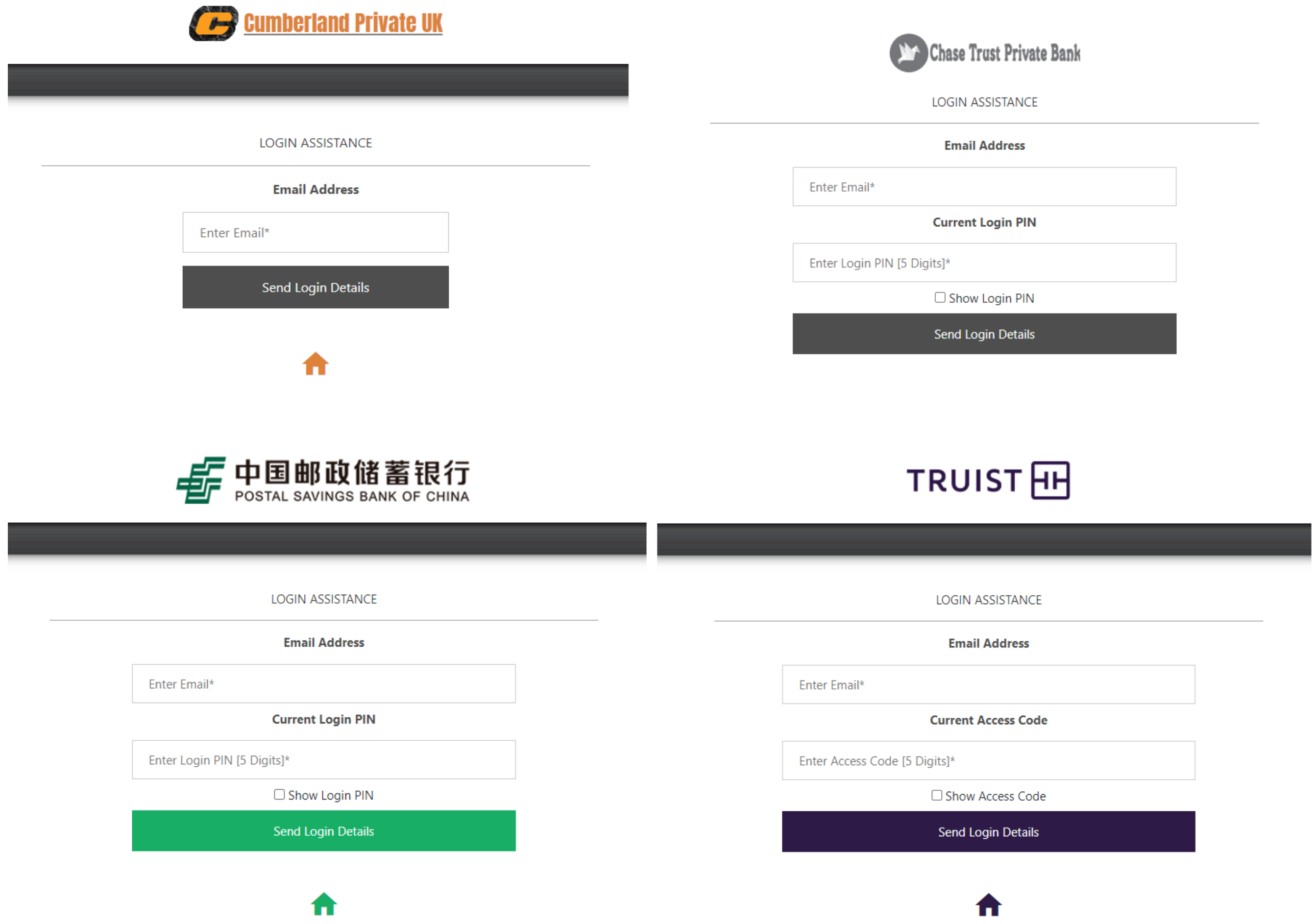
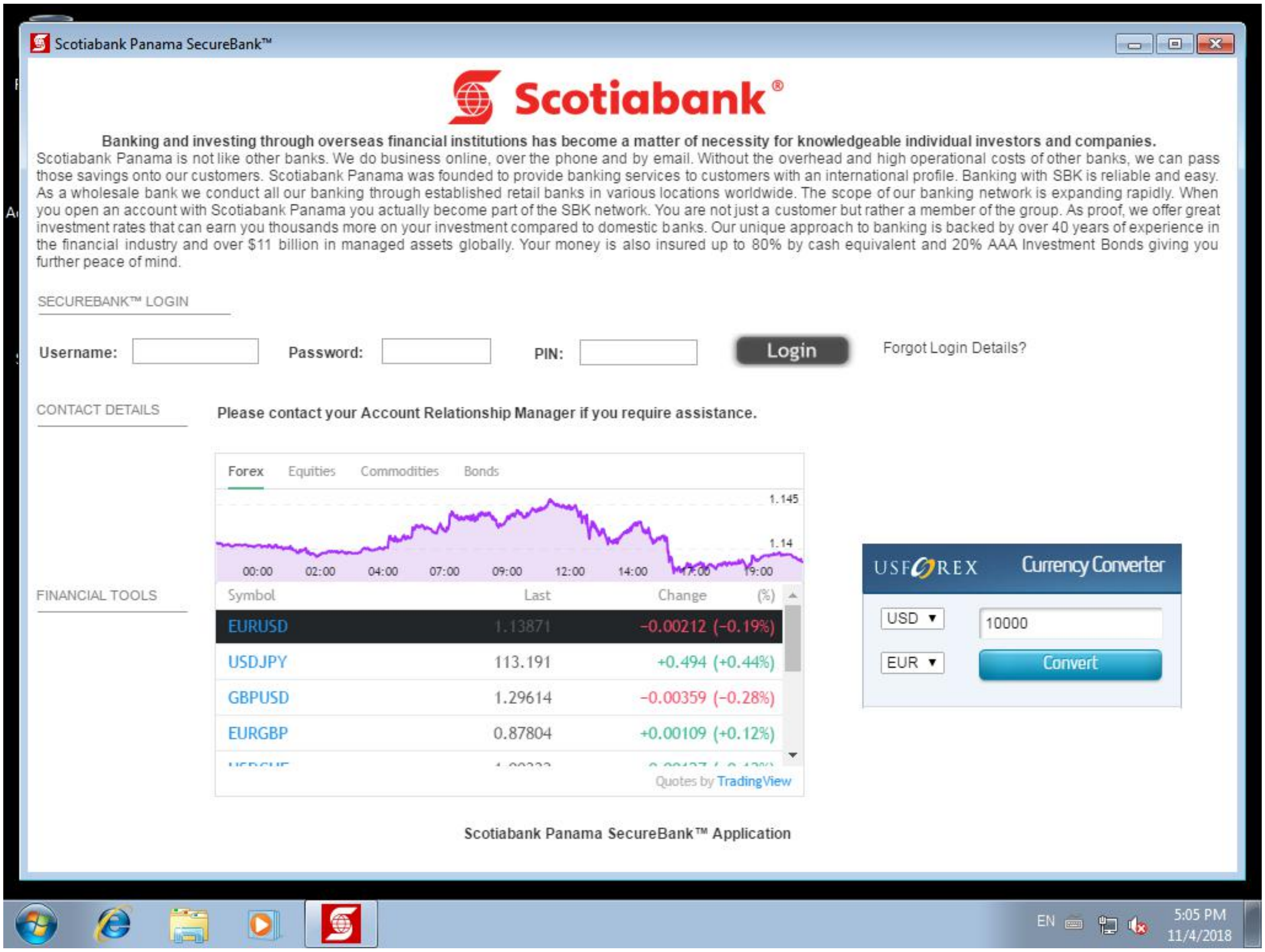


Fig. 2 – Fake login pages with identical forms but alternative logos used by the threat actors.

This investigation uncovered additional fake login pages posing as other investment banks, including Cumberland Private Wealth, Truist, First National Bank of America, MayBank Private Malaysia, Central Bank of West African States (BCEAO), Chase Trust, and the Postal Savings Bank of China, BNY Mellon, Scotiabank Panama, Multibank Panama, BB&T, and MetroBank.

Pivoting from these additional domains and IP addresses revealed other fake Windows applications that had been used by the attackers to deliver a backdoor. As summarised in the initial advisory, the attackers send an email to the target containing a URL and login credentials for a fake website. When these credentials are used to enter the site, the victim downloads an installer which unpacks a ZIP file. This delivers the backdoored application which, if executed by the user, provides remote access to the device.



Scotiabank Panama SecureBank™

Scotiabank®

Banking and investing through overseas financial institutions has become a matter of necessity for knowledgeable individual investors and companies.

Scotiabank Panama is not like other banks. We do business online, over the phone and by email. Without the overhead and high operational costs of other banks, we can pass those savings onto our customers. Scotiabank Panama was founded to provide banking services to customers with an international profile. Banking with SBK is reliable and easy. As a wholesale bank we conduct all our banking through established retail banks in various locations worldwide. The scope of our banking network is expanding rapidly. When you open an account with Scotiabank Panama you actually become part of the SBK network. You are not just a customer but rather a member of the group. As proof, we offer great investment rates that can earn you thousands more on your investment compared to domestic banks. Our unique approach to banking is backed by over 40 years of experience in the financial industry and over $11 billion in managed assets globally. Your money is also insured up to 80% by cash equivalent and 20% AAA Investment Bonds giving you further peace of mind.

SECUREBANK™ LOGIN

Username: Password: PIN:

CONTACT DETAILS

Please contact your Account Relationship Manager if you require assistance.

FINANCIAL TOOLS

Symbol	Last	Change (%)
EURUSD	1.13871	-0.00212 (-0.19%)
USDJPY	113.191	+0.494 (+0.44%)
GBPUSD	1.29614	-0.00359 (-0.28%)
EURGBP	0.87804	+0.00109 (+0.12%)

USD ▾ 10000

EUR ▾

Scotiabank Panama SecureBank™ Application

Fig. 3 – Fake Windows application impersonating Scotiabank Panama.

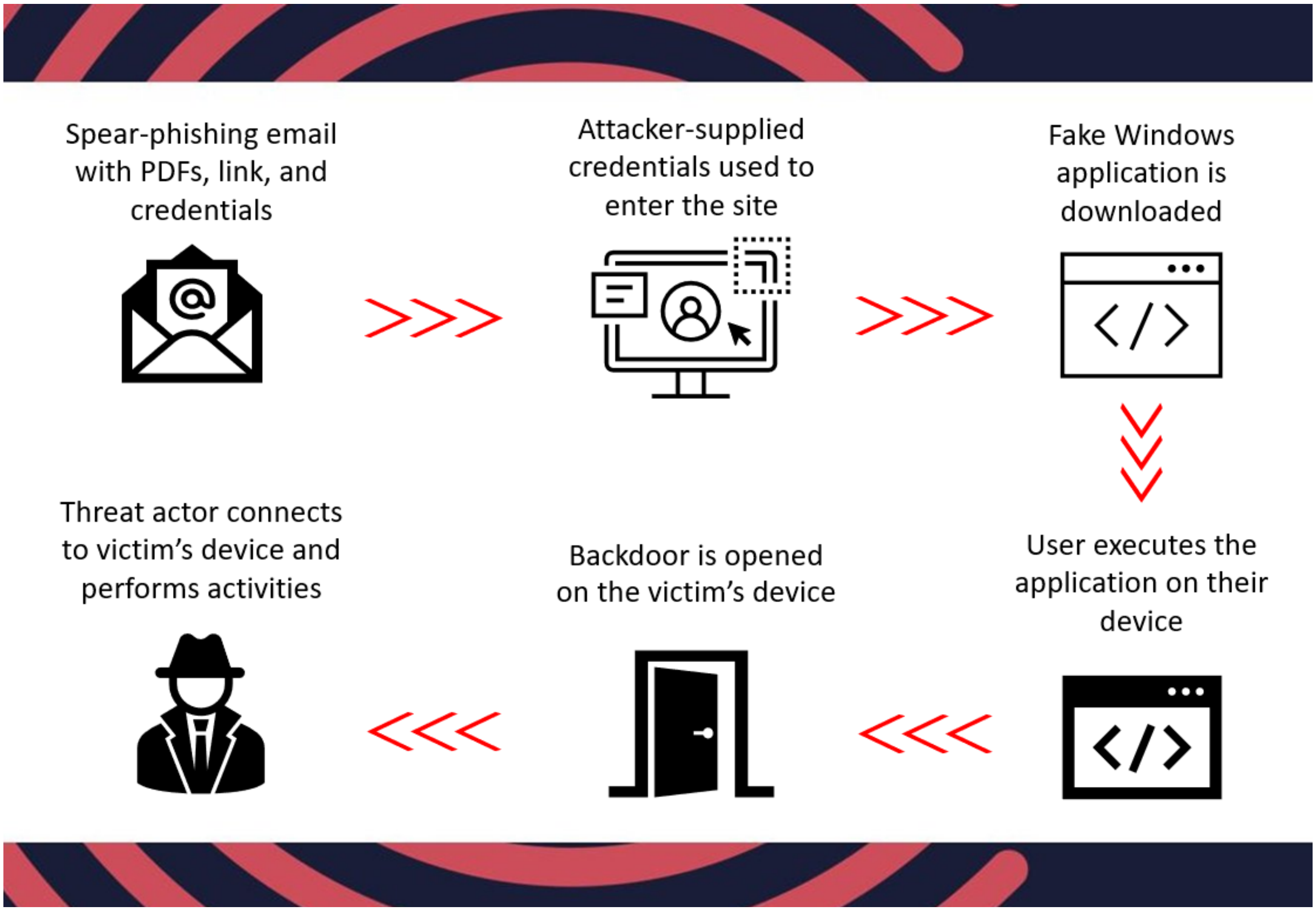

Spear-phishing email with PDFs, link, and credentials
Attacker-supplied credentials used to enter the site
Fake Windows application is downloaded
User executes the application on their device
Backdoor is opened on the victim's device
Threat actor connects to victim's device and performs activities

Fig. 4 – Infection chain diagram depicted by Cyjax analysts

Further analysis of the malicious campaign infrastructure exposed several patterns:

- All the domains hosted with either Secured Servers (AS20454) or Host Winds (AS54290) and Interserver Name Servers (AS19318)
- The attackers either used the ".com" TLD or ".online" gTLD to create lookalike domains to impersonate the investment banks
- The Windows applications appear to have been built with an open-source project on GitHub called Squirrel (available here)
- The Windows applications are large files, at around 42MB in size, with very low detection ratings on VirusTotal
- The Windows applications likely inherited RAT functionality from TeamViewer, a legitimate remote admin tool often used by threat actors

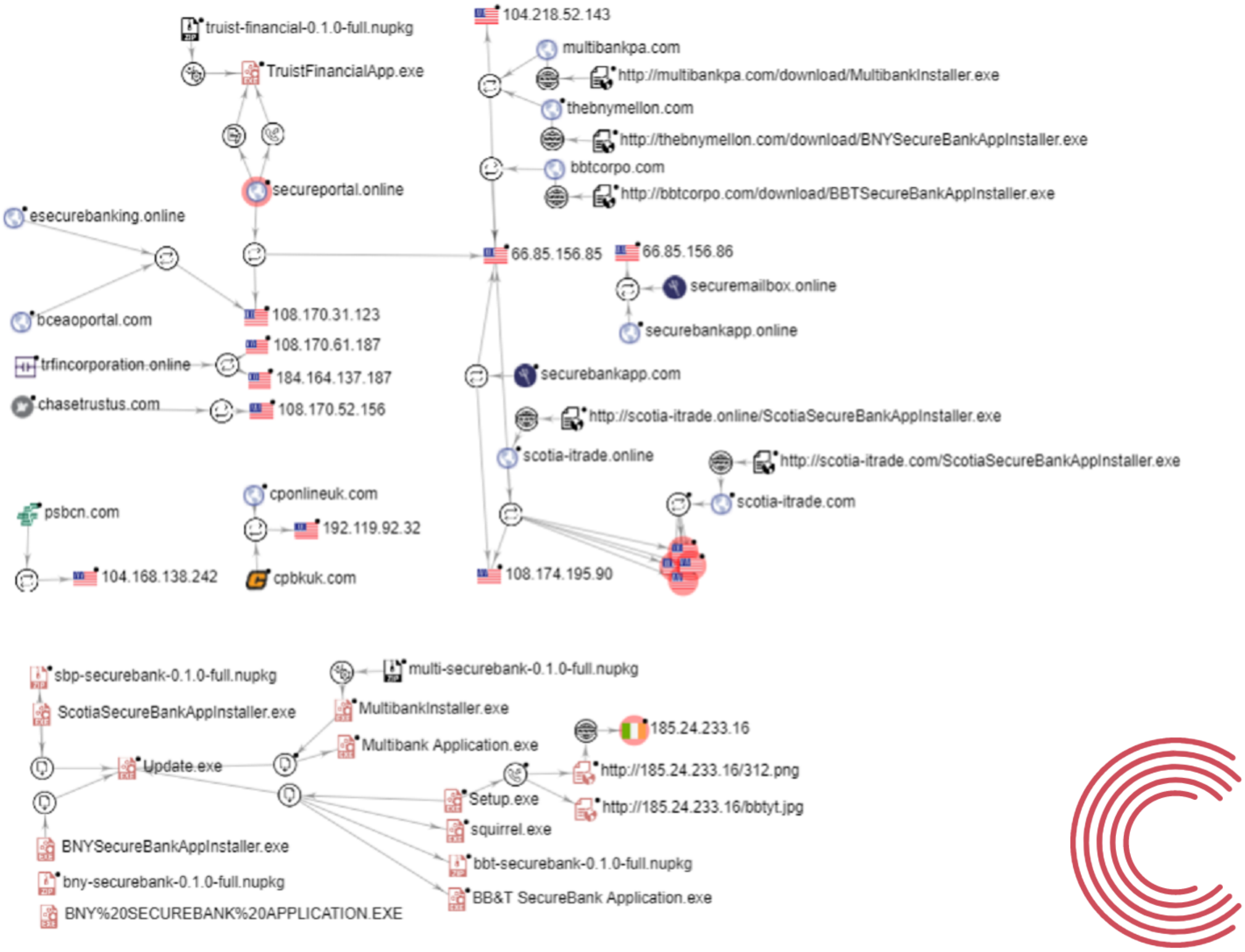

truist-financial-0.1.0-full.nupkg
TruistFinancialApp.exe
secureportal.online
esecurebanking.online
bceaoportal.com
108.170.31.123
trfincorporation.online
108.170.61.187
184.164.137.187
chasetrustus.com
108.170.52.156
104.218.52.143
multibankpa.com
http://multibankpa.com/download/MultibankInstaller.exe
thebnymellon.com
http://thebnymellon.com/download/BNYSecureBankAppInstaller.exe
bbtcorpo.com
http://bbtcorpo.com/download/BBTSecureBankAppInstaller.exe
66.85.156.85
66.85.156.86
securemailbox.online
securebankapp.online
securebankapp.com
http://scotia-itrade.online/ScotiaSecureBankAppInstaller.exe
scotia-itrade.online
http://scotia-itrade.com/ScotiaSecureBankAppInstaller.exe
scotia-itrade.com
psbcn.com
104.168.138.242
cponlineuk.com
192.119.92.32
cpbkuk.com
108.174.195.90
sbp-securebank-0.1.0-full.nupkg
ScotiaSecureBankAppInstaller.exe
Update.exe
multi-securebank-0.1.0-full.nupkg
MultibankInstaller.exe
Multibank Application.exe
185.24.233.16
http://185.24.233.16/312.png
http://185.24.233.16/bbtyt.jpg
Setup.exe
squirrel.exe
bbt-securebank-0.1.0-full.nupkg
BB&T SecureBank Application.exe
BNYSecureBankAppInstaller.exe
bny-securebank-0.1.0-full.nupkg
BNY%20SECUREBANK%20APPLICATION.EXE

Fig. 5 – Graph of the campaign infrastructure using VirusTotal

Interestingly, the same servers used by the attackers also hosted several domains impersonating the FBI, Europol, HM Revenue & Customs, the Bank of England, US Federal Reserve, US Treasury, and the World Bank. It is currently unclear if these domains are connected to the same campaign: we found no emails, login pages, or samples using them. However, it remains a significant finding because it is of a piece with these threat actors' TTPs – the FBI disclosed the threat actors masqueraded as the UK National Crime Agency in one of the PDFs attached to an email.

This highly targeted campaign has yet to be attributed to a known APT or cybercriminal group. Its success rate is currently unknown, but the campaign combines multiple techniques corresponding to somewhat sophisticated cybercriminals, making it a serious threat. Using the information harvested from backdoored systems, the attackers can access their victims' accounts and various other sensitive data to further compromise the target networks or steal more funds.

Using fake applications as decoys while performing malicious activity in the background is a common tactic: it has been employed by cybercriminals and state-backed financially motivated threat actors, such as the Lazarus group. The North Korean APT used its AppleJeus malware to target hundreds of organisations in over 30 countries during 2020. It used backdoored applications that provided initial access to its victims' networks to steal cryptocurrency from their virtual wallets. The earliest versions appeared in 2018. In this campaign, the initial infection vectors included spear-phishing via emails, malicious links sent via social media, and other social engineering techniques. [5, 6]

IOCs

Type	Indicator	Name
EXE	e09ae3c1ff5489f300ec9ecfc76ffdab90b6dab07eff1a0edf38285ab1e2b801	TruistFinancialApp.exe
NuGet (NUPKG)	b5ab061ae764c10896d5889ac241d94aa50d2b5713c15e3b23e7c23454296bef	truist-financial-0.1.0-full.nupkg
EXE	49b71bf037995e26819d36c11f7ab8cbd8c2ab58155c6ad4786996fd42994213	BNYSecureBankAppInstaller.exe

Type	Indicator	Name
NuGet (NUPKG)	97e21c919783cd645f6237064277a8c4b97245915fa3bfd7d8888004a7858b91	bny-securebank-0.1.0-full.nupkg
EXE	344540bc935624cbdc21e51478f061a7e98fce0b5c0082e0e14c33e502833a80	BNY%20SECUREBANK%20APPLICATION.EXE
EXE	f46ae7989893a150a0620206ed8d8bfad17b2b542b9f9e599d683da272ab2ce0	ScotiaSecureBankAppInstaller.exe
NuGet (NUPKG)	da849c361e3e6284ea0ec7a35c3834473682f27755dd1962b520a0d42f423b66	sbp-securebank-0.1.0-full.nupkg
EXE	6f6e630ec432e7b559d5d7dcb8ecd88223857cdd3bb863bd597fecde03031a8c	MultibankInstaller.exe
NuGet (NUPKG)	3cd6061599887ed296ae32e24ae9ccc6433359b0c40ffb882d7cdf0884cd5552	multi-securebank-0.1.0-full.nupkg
EXE	e9c6f21f59c3d498d8f92a00596b461756e22f19cf42d5e5bd3e9b938fd84323	Multibank Application.exe
EXE	0589f1c49f55ccfffbbf40b2a1e516cbee14c42896d5641cc500f978fc7eab99	Setup.exe
NuGet (NUPKG)	0f784a5e5daeffec55350213ec6f9dba7834935a77913bfb8fb8866122499b5a	bbt-securebank-0.1.0-full.nupkg
EXE	0754d1de2deeca3062d62489a0c15255ab3eb2411d513ec7126f01eb98dbf85a	BB&T SecureBank Application.exe
EXE	2e4af4ffcbb2e5c49a44596ed423e8c3213884daba74a051a75afed9abbbc047	MetroBankInstaller.exe
URL	hxxp://thebnymellon[.]com/download/BNYSecureBankAppInstaller.exe	
URL	hxxp://scotia-itrade[.]online/ScotiaSecureBankAppInstaller.exe	
URL	hxxp://scotia-itrade[.]com/ScotiaSecureBankAppInstaller.exe	
URL	hxxp://multibankpa[.]com/download/MultibankInstaller.exe	
URL	hxxp://bbtcorpo[.]com/download/BBTSecureBankAppInstaller.exe	
URL	hxxps://secureportal[.]online/securebank/forgotpassword/passwordlogin.html	
URL	hxxps://secureportal[.]online/truistonline/forgotpassword/passwordlogin.html	
URL	hxxps://secureportal[.]online/truistapp/app/index.html	
URL	hxxps://secureportal[.]online/fbnusa/forgotpassword/passwordlogin.html	
URL	hxxps://secureportal[.]online/mayprivateonline/forgotpassword/passwordlogin.html	
URL	hxxps://www[.]bceaoportal[.]com/cnbonline/forgotpassword/passwordlogin.html	
URL	hxxps://www[.]cpbkuk[.]com/securebank/forgotpassword/passwordlogin.html	
URL	hxxp://chasetrustus[.]com/chasetrustus/forgotpassword/passwordlogin.html	
URL	hxxp://psbcn[.]com/eng/psbcnonline/forgotpassword/passwordlogin.html	
URL	hxxps://trfincorporation[.]online/truistonline/forgotpassword/passwordlogin.html	