# Resecurity | BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2,5M in Demands

Published: 2022-07-10 · Archived: 2026-04-05 13:01:38 UTC

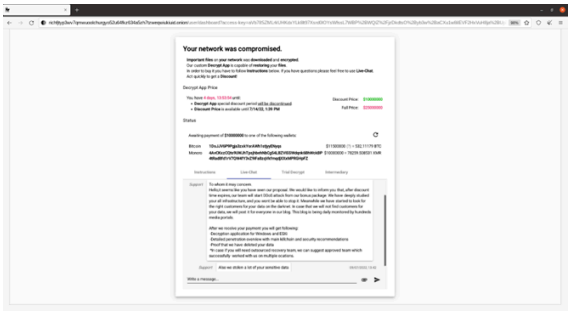
*The notorious cybercriminal syndicate competes with Conti and Lockbit 3.0. They introduced an advanced search by stolen victim's passwords, and confidential documents leaked in the TOR network.*

Resecurity (USA), a Los Angeles-based cybersecurity company protecting Fortune 500 companies, has detected a significant increase in value of ransom demand requests by the notorious BlackCat ransomware gang. Such tactics significantly affect ransomware underground ecosystems, hitting businesses of different sizes hard worldwide. Based on the recently compromised victims in Nordics region, which haven't been disclosed by the group yet, the amount to be paid exceeds $2 million.

BlackCat has been operating since at least November and has launched major attacks such as in January the disruption of OilTanking GmbH, a German fuel company, and in February, the attack on an aviation company, Swissport. Most recently, the ransomware group claimed responsibility for attacks against two universities in the U.S., Florida International University, and the University of North Carolina A&T.

According to experts from Resecurity, BlackCat ransomware actors began defining $2,5 million ransom demands, with a possible discount close to half, motivating the victim to resolve the incident as soon as possible. The average time allocated for payment varies between 5-7 days, to give victim some time to purchase BTC or XMR cryptocurrency. In case of difficulties, the victim may engage an "intermediary" for further recovery process.

The average ransomware payment climbed 82% since 2020 to a record high of $570,000 in the first half of 2021, and then by 2022 it almost doubled. The latest forecast is for global ransomware extortion activity to reach $265 billion by 2031, with total damages for businesses valued at $10,5 trillion globally. Such metrics would make ransomware the world's largest "shadow economy", generating more damage in expenses than natural disasters. Unfortunately, despite guidance of DOJ not to pay ransom, over 48% of the impacted organizations had to pay cybercriminals due to no alternative options available to recover their operations timely.

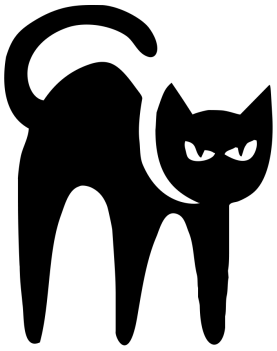



Example of Blackcat ransomware payment landing page with the deadline of payment by July 14th

BlackCat ransomware is one of the fastest-growing Ransomware-as-a-Service (RaaS) underground groups practicing so called "quadruple extortion" pressing victims to pay:

1. **Encryption:** Victims pay to regain access to scrambled data and compromised computer systems that stop working because key files are encrypted.
2. **Data Theft:** Hackers release sensitive information if a ransom is not paid. As proof, the bad actors share an example of the stolen data or send a listing of stolen files to avoid any legitimacy doubts.
3. **Denial of Service (DoS):** Ransomware gangs launch denial of service attacks that shut down a victim's public websites.
4. **Harassment:** Cybercriminals contact customers, business partners, employees, and media to tell them the organization was hacked.

The BlackCat is also known as "ALPHV", or "AlphaVM" and "AphaV", a ransomware family created in the Rust programming language. In April the FBI published a flash alert about BlackCat ransomware naming the group as one of the top ransomware threats. The name "BlackCat" is coming from a specific icon used in the landing page for ransom payment:



Notably, despite the fact BlackCat and Alpha have completely different URLs in TOR Network, the scenarios used on their pages are identical, and likely developed by the same actors.

http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion

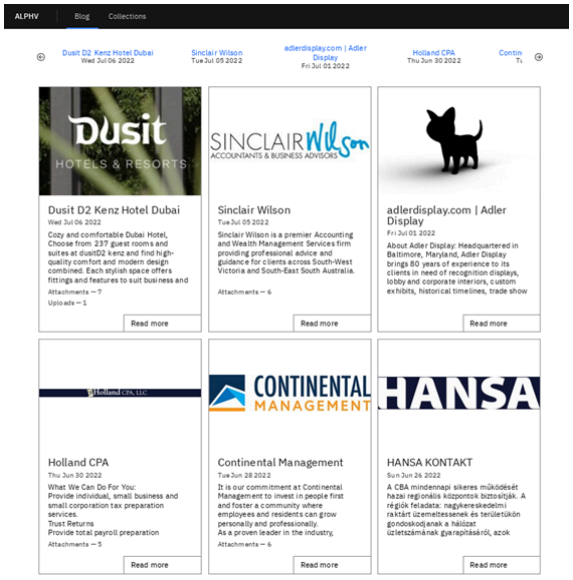

http://wnlwdb6yumubpjwpnwvek6qs4mpudmhy7tyulaqbxmztgreobaevqkid[.]onion


The URL used for victim landing page typically includes symbols "access key".

http://richfjtyp3wv7qmwuoolchurgyo52u64fkz634a5zh7tzweqwiukiuid.onion/?access-key=

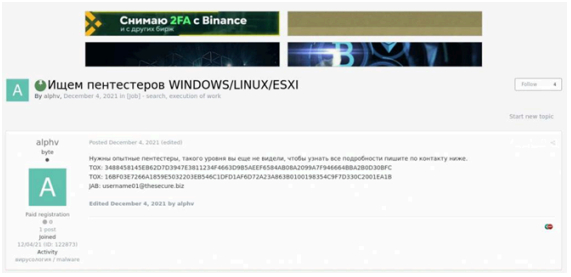
Today the group published new victims - COUNT+CARE Gmbh (an information technology and services company from Germany), following Dusit D2 Kenz Hotel in Dubai, Sinclair Wilson (an accounting and wealth management services firm from Australia) and Adler Display out of Baltimore, Maryland.

Japanese gaming giant Bandai Namco and aerospace sensor Maker Hydra-Electric from Burbank, California.



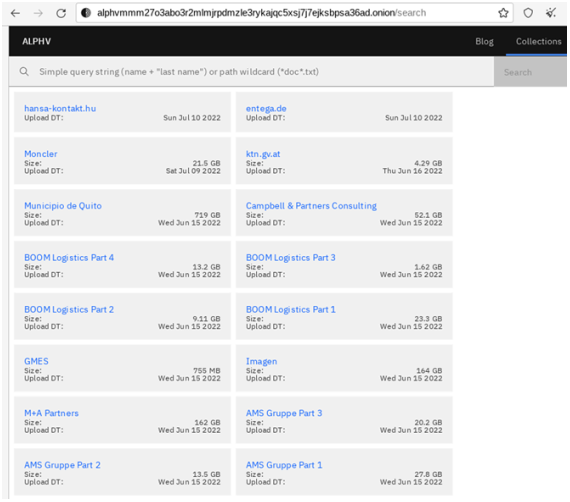

The group is publishing new victims almost every 4 days. Notably, there is a certain difference between BlackCat and AlphV in their ‘modus operandi’ of the extortion techniques – the last is publicly shaming victims by using their resource in the TOR network, while the first one - remains low-key and stealth attacking high-profile targets without further significant disclosure.

December 4, 2021 – AlphV published a posting in Dark Web, searching for experienced penetration testing specialists to compromise targets of interest. They published 2 TOX IM contacts and Jabber:

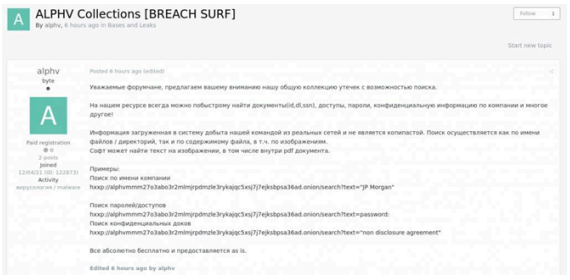



Based on the analysis of the latest incidents, BlackCat adds a randomized 6 symbols extension, for e.g. ".sxuetaf”, after file encryption similar Lockbit (7 symbols), NetWalker (6 symbols) and Locky ransomware (5 symbols). Notably, there were identified multiple victims by Blackhat having 7 symbols extension as Lockbit 2.0 strain.

The actors were one of the first who introduced “search” in a leaked data. It allows employees and customers of the affected company to check if their data has been exposed.




In a recent post from 10 Jul 2022, 15:35 pm in Dark Web, the group introduced search not only by text signatures, but also supporting tags for search of passwords and compromised PII




**Translation:**

*Dear forum users, we want to introduce you our repository of leaks with search feature.*

*On our resource you may always quickly find documents (IDs, DL, SSN), access credentials, passwords, confidential information by company name, and a lot more!*

*Information imported into the system has been acquired by our team from the real victims' networks. The search can be performed by name of the file/folders, but also content (of the file), including images. The tool will find text recognized on the image, including in the body of PDF document.*

**Examples:**

***- Search by the name of the company (victim):***

*alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/search?text="JP Morgan"*

***- Search of passwords:***

*alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/search?text=password:*

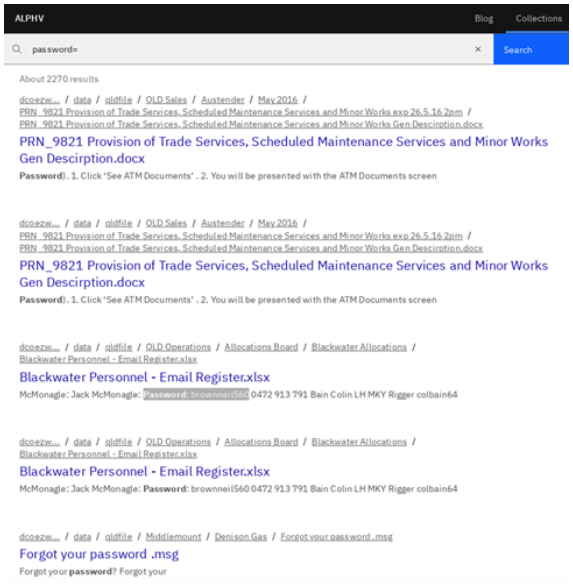
***- Search of confidential documents***

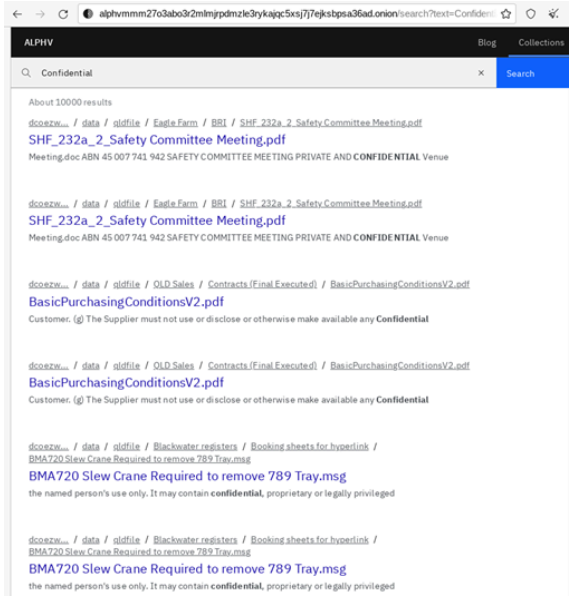
*alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion/search?text=”non disclosure agreement”*

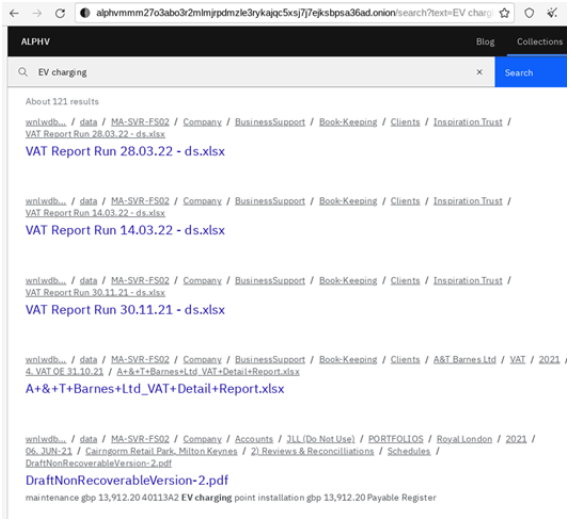
*Everything is absolutely for free and “as is”.*

It seems to be that some of the stolen files are still under indexing, but majority is already available for quick navigation.


There were over 2,270 indexed documents identified containing access credentials and password information in plaintext, and over 100,000 documents containing confidential marking.






ALPHV seems to be significantly competing with LOCKBIT and CONTI – another actively developing ransomware syndicates who called ALPHV “scammers”. Likely, the statement was related to some conflict and issues between initial access brokers (IABs), affiliates and team members who could be associated with both projects at different stages.

ALPHV has been associated with two other ransomware groups: DarkSide and BlackMatter. Design overlaps between ALPHV and DarkSide have prompted rumors that ALPHV was a rebrand of DarkSide following the latter’s high-profile attack on the Colonial Pipeline.

On underground cybercriminal forums, the representative of the “LockBit” ransomware also initiated threads to state that ALPHV was a rebrand of DarkSide and BlackMatter RaaS programs. While ALPHV denied to be a rebrand of DarkSide or BlackMatter, developers and money launderers from ALPHV are linked to DarkSide/BlackMatter, according to the FBI. Therefore, while ALPHV may not be a rebrand, it is likely that the group recruited many members from these now inactive ransomware gangs.

One of the first public appearances of ALPHV occurred on the RAMP cybercriminal forum on 09 Dec 2021, where a representative of the group promoted the ALPHV RaaS program and attempted to recruit affiliates. In this post, ALPHV operators advertised the new “ALPHV-ng (New Generation)” RaaS partner program, which they described as the next generation of ransomware. The ransomware had been written from scratch and have many features, including:

- Four encryption modes: full, fast, DotPattern, and Auto. It uses the two encryption algorithms ChaCha20 and AES.
- Infrastructure fragmented with nodes that are interconnected and located behind “NAT + FW”. The infrastructure is set up so that attackers will not reveal the real IP addresses of their servers when receiving cmdshells.
- Functional on different platforms including various versions of Linux (ESXI, Debian, Ubuntu, and ReadyNas) and all versions from Windows 7 and above.
- Generated “a unique onion domain” for “each new victim”.

Resecurity’s HUNTER unit noticed significant developments on RAMP forum (ransomware underground community) and expects to see more activity from competing groups including Lockbit 3.0.

Actors involved in the ransomware business are trying to isolate themselves from semi-public or well-recognized Dark Web forums, they're doing this to create a community of vetted initial access brokers, developers of ransomware, and actors involved in other related operations.

## MITRE ATT&CK:

[T1592] Gather Victim Host Information
[T1586] Compromise Accounts
[T1490] Inhibit System Recovery
[T1590] Gather Victim Network Information
[T1486] Data Encrypted for Impact
[T1040] Network Sniffing
[T1133] External Remote Services
[T1098] Account Manipulation
[T1053] Scheduled Task/Job
[T1078] Valid Accounts
[T1484] Domain Policy Modification
[T1222] File and Directory Permissions Modifications
[T1036] Masquerading
[T1003] OS Credentials Dumping
[T1528] Steal Application Access Token
[T1558] Steal or Forge Kerberos Tickets
[T1212] Exploitaton for Credentials Access
[T1555] Credentials from Password Stores
[T1482] Domain Trust Discovery
[T1083] File and Directory Discovery
[T1615] Group Policy Discovery
[T1072] Software Deployment Tools
[T1020] Automated Exfiltration
[T1048] Exfiltration over Alternative Protocol
[T1537] Transfer Data to Cloud Account

## Tooling:

BlackCat arsenal employs multiple tools for network intrusions and post-exploitation targeting Active Directory including but not limited to:

- ADRecon, network reconnaissance tool for Windows environment;
- Cobalt Strike, post-exploitation framework;
- PsExec tool for lateral movement in the victim's network;
- Mimikatz, the well-known hacker software;
- Nirsoft software to extract network passwords.

Due to a significant number of affiliates and independent initial access brokers (IABs) collaborating with BlackCat group, the tooling may vary. As the most commonly seen in the result of DFIR engagements:

- Bloodhound tool
- Softperfect Netscan
- CrackMapExec
- Inveigh/InveighZero
- MegaSync
- RClone
- Adfind
- Rubeus
- Stealbit

ExMatter, an exfiltration tool that has earlier been seen in the arsenal of BlackMatter affiliates

Some of these tools are packaged and dropped on the victim's machine in form of dropper (.bat or PowerShell scenario).

### Tactics & Procedures:

While the approach used by BlackCat is not unique, and widely used by other actors attacking enterprise networks, the following aspects may be relevant to Ransomware activity:

- Using SysVol Share to store BlackCat Cryptor (locker) to replicate it across other hosts within the same Active Directory domain;

- The malware usnice.

es Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware.

- Active exploitation of CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523 to target Microsoft Exchange.

- Evasive tactics, such as masking a tampered DLL to make it seem legitimate.

- Before the encryption process, the actors perform comprehensive preparation to prevent possible roll-back to normal operations from possible backups stored in the network.

In Linux environments once initial access is obtained, actors establish reverse SSH tunnels as a command-and-control (C2) channel between victims and BlackCat infrastructure.

### Known TOR nodes:

alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.onion]
jjeqizt46yqydabjkdkfsiptzfzcbzjkcaou77v7ljoxgsyg3e5luqqd[.onion]
pmpkjv36ca5ykwmjnfnr5cadctt4ldcekaxocbwa57btujhi7mly6kid[.onion]
hzdpwv5jqjcbstv5kassyxztdkacwi4ucleomgpqmxcwan5ydzqh5mid[.onion]
id7seexjn4bojn5rvo4lwcjgufjz7gkisaidckaux3uvjc7l7xrsiqad[.onion]

sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd[.onion]
htnpafzbvddr2llstwbjouupddflqm7y7cr7tcchbeo6rmxpqoxcbqqd[.onion]
aoczppoxmfqqthtwlwi4fmzlrv6aor3isn6ffaiic55wrfumxslx3vyd[.onion]
5e2q3uzczl3bur23dxfxxu5unlukuqrlseesmxc7v7dmo4qgbr3kaxqd[.onion]
vldmvht6s253et33ce6gcth2vikuvsi7xgkzim5frqiowq6an6tmlaad[.onion]
kxmbveamxzfrnxacprpbldcy3p263kvrjiblaw4p55mzrkaf3si6w4id[.onion]
doh3rlqtvg24yu4r4w7bk5twm7w6nm7wqsr3d3roc7jisrdqf5catnad[.onion]
dcoezwwwxij2trzd3oqhtyjg3lgvgzmyzrj2pcs3rdfh4tl5267dwpyd[.onion]
s5hcgpxzeehnkwlpb3xkelvkv6rpi5rszmhfeywncja26bxdzexp6zqd[.onion]
oylk6phjrgcjvhv5rjijwrpcqj4ig3f2evbxb6lzofw7cbgxlpetq7ad[.onion]
fbehz3443h644jrcu3djvexhplhmnijilkq54puzrxuvloc42oykgiad[.onion]
kv7nxc6sg625vl4rd4fsy4asero3jqivp7zyhaohsyww2xnk7r7yenyd[.onion]
acvhxy4cc52a7iv7ugc4eq6dq6nus2s5xduew7s2wkaw6nhftasyq2yd[.onion]
wnlwdb6yumubpjwpnwvek6qs4mpudmhy7tyulaqbxmztgreobaevqkid[.onion]
zf3raijx7m6xm72uenqrql5b2qtkbvnxi7fgzqjxfcizp7lylmvzvdid[.onion]
smo3gebcr5mkff7ja5ayi2xdz2xsapdixak4eosj5ah6fgrbluoxrkqd[.onion]
2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid[.onion]
vqifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd[.onion]
jrq44df5h2xysjsajuidspv7zxl7g7v7viujicudptufaozi2i65cnad[.onion]
cfj4bsnfi4ktpfoei7uqggz5sb443fhvvbkxbmu3dhfriomg2txxgxid[.onion]
zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd[.onion]
s7isfnfsrrnogkkvzzmqpqlcehajalaht5nmel7nbxwhvqc52jj2ejid[.onion]
mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd[.onion]

## IOCs:

f815f5d6c85bcbc1ec071dd39532a20f5ce910989552d980d1d4346f57b75f89
c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40
74464797c5d2df81db2e06f86497b2127fda6766956f1b67b0dcea9570d8b683
4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf
1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e
15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed
13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31
c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283
bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117
7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487
38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1
2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc
28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169
0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479
f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f

3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83
7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e
cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae

## Mitigation Strategies:

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system defined or recognized scheduled tasks for unrecognized “actions” (for example: review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multifactor authentication where possible.
- Regularly change passwords to network systems, accounts, and avoid reusing passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update antivirus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

---