RIZE
TECHNOLOGIES

GALACTIC
ADVISORS

REPORT OF FINDINGS

RIZE TECHNOLOGIES

GALACTIC ADVISORS

Results for:

BACKUPS

ACCOUNTS

M365

PATCHES

ANTIVIRUS

FIREWALLS

EDUCATION

ENCRYPTION

SURVEILLANCE

REPORT OF FINDINGS

Results for:

[redacted]

BACKUPS

ACCOUNTS

M365

PATCHES

ANTIVIRUS

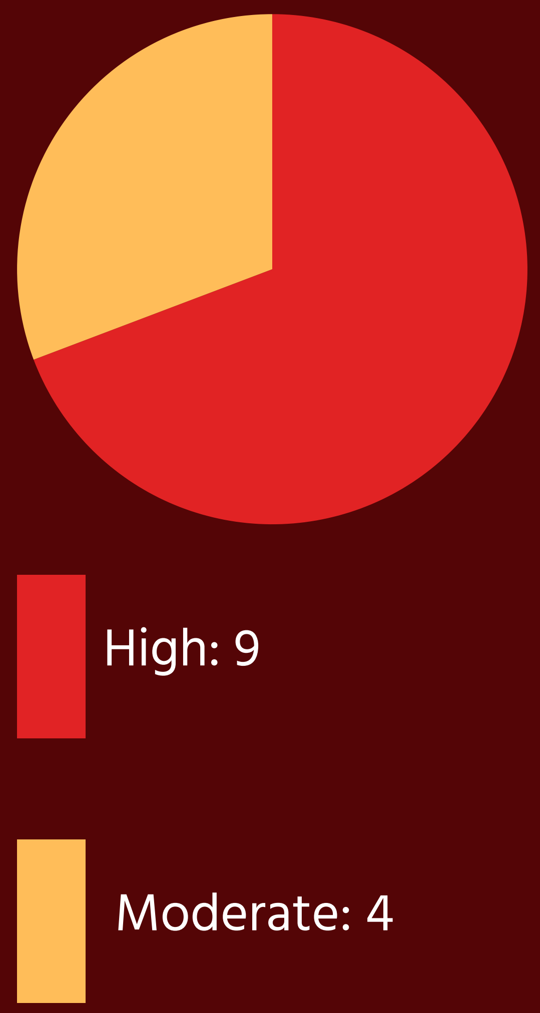
FIREWALLS

EDUCATION

ENCRYPTION

SURVEILLANCE

RISK BREAKDOWN



METHODS

Penetration test - Reasoning/Methodology

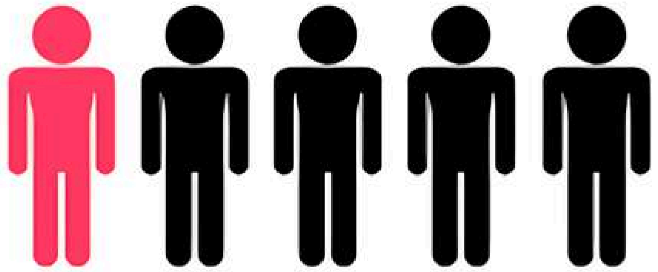
Do you know WHY users are your biggest cybersecurity threat? Because studies show that 91% of ALL cyberattacks start with a phishing email. This puts the hacker right inside your organization. Our team uses a proprietary (patent pending) process to go beyond phishing training and find our what a hacker can gain access to when someone in your organization is phished.

Internal Testing - Considering over 90% of cyberattacks begin with a phishing email and over 19.8% of employees click phishing email links, our team focuses on what the attacker will gain access to if a normal user were to click on a link. We target employees who are the most likely to be phished. These employees also happen to be the ones who have the most to lose: CEOs, CFOs, Directors, HR, and sales team members. Why are they more likely to be phished in the first place? They are often communicating with people outside your organization AND they process many more emails than others.

External Testing - What about the other 9% of attacks, how do they get started? Hackers build sophisticated automation that is constantly scanning the internet looking for vulnerabilities. They use these vulnerabilities to get into networks. We use some of the same tactics to outline the perimeter of your organization, look for exposed services, find vulnerabilities, and attempt to exploit them.

The following report contains evidence of our findings, remediation steps, as well as descriptions of the risks associated with them.

Hackers are constantly coming up with new attack chains and vulnerabilities. These new methods need to be evaluated and remediated often. Best practice includes regular ongoing security assessments to identify and respond to these new threats.



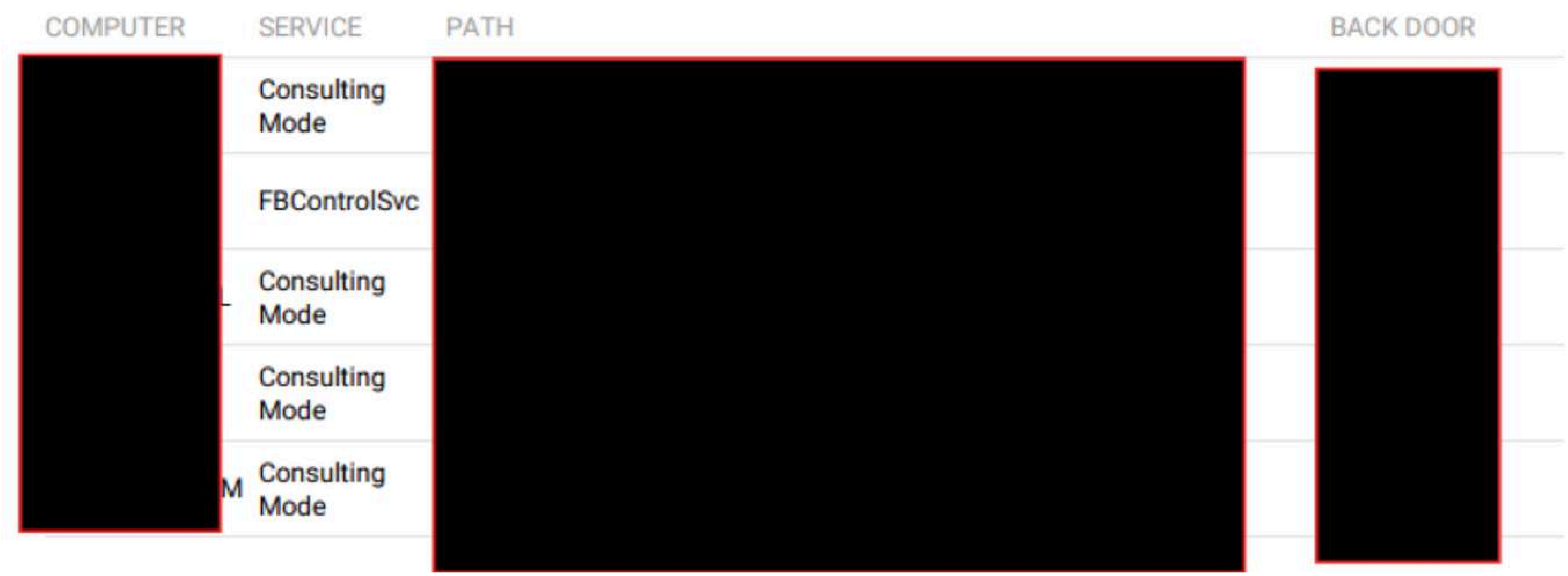
19.8% OF EMPLOYEES CLICK ON PHISHING LINKS

91% OF CYBERATTACKS BEGIN WITH A PHISHING EMAIL

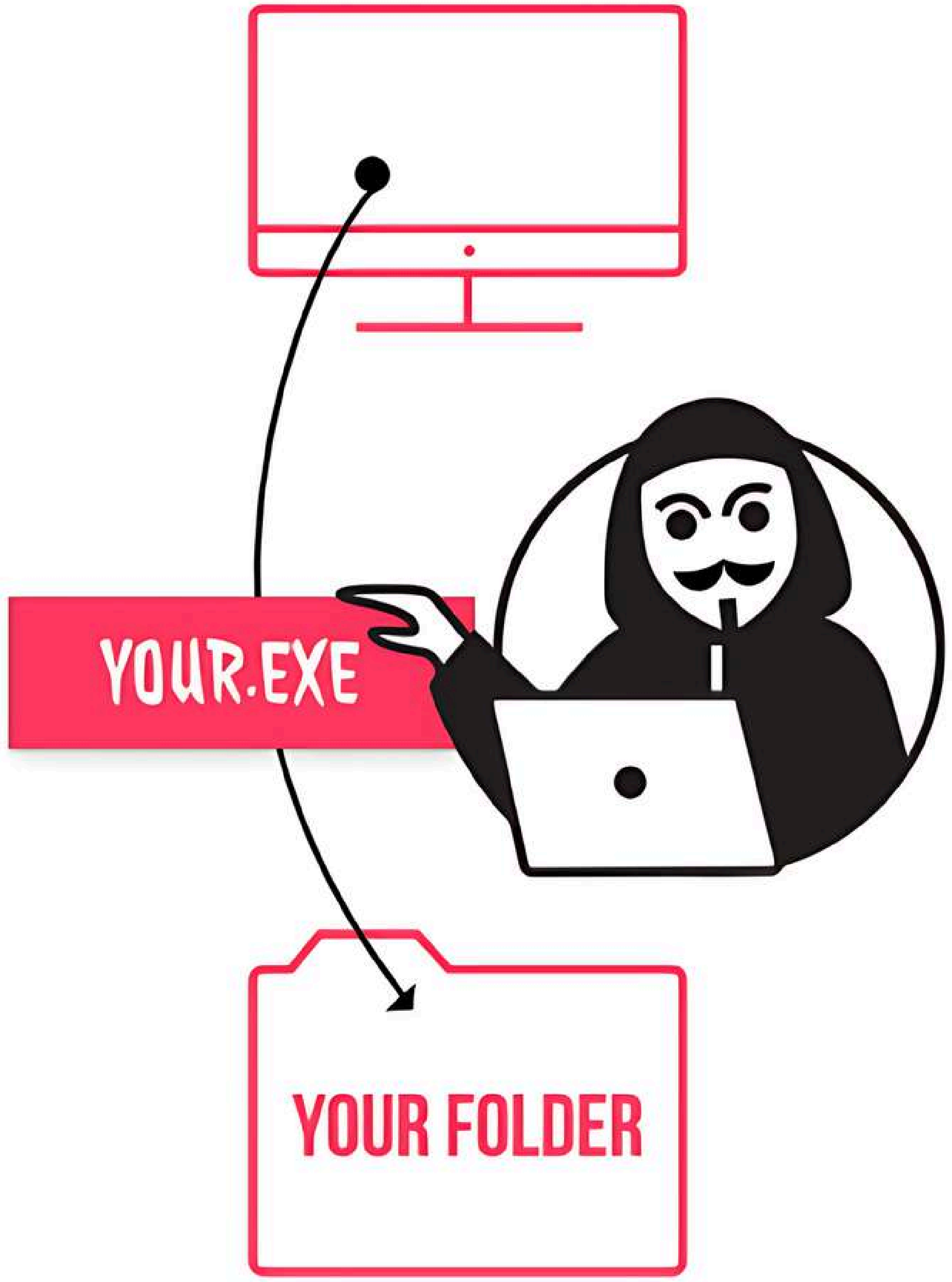
METHODS HIGH RISK ISSUES

IMPROPERLY ESCAPED SERVICE FILE PATH

Hackers use service paths like this to insert executables in the file path to allow them to gain service level or administrative level access to a device. This provides a way for the attacker to simply phish a user and gain additional access to the network or other resources that the normal user has rights to access.



COMPUTER	SERVICE	PATH	BACK DOOR
[redacted]	Consulting Mode	[redacted]	[redacted]
[redacted]	FBControlSvc	[redacted]	[redacted]
[redacted]	Consulting Mode	[redacted]	[redacted]
[redacted]	Consulting Mode	[redacted]	[redacted]
[redacted]	Consulting Mode	[redacted]	[redacted]



Remediation: Add quotes to the services listed above so they are properly escaped and an attacker cannot insert malicious code into the path, restart the service and gain system level access.

BACKUPS

BACKUP RESTORE TESTING NOT SUFFICIENT

Without a test restore, there is no evidence the backup is capable of being restored. Testing the recovery process is a critical part of backing up data. This information is needed to validate the amount of time a restore will take.

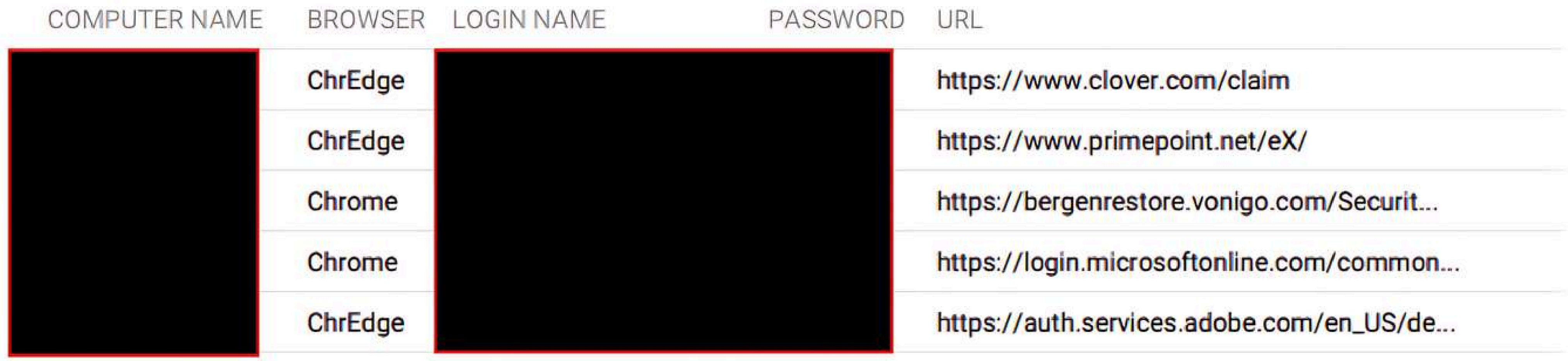
Remediation: Restore testing should happen on at least a monthly basis.

ACCOUNTS HIGH RISK ISSUES

PASSWORDS CRACKED SUMMARY

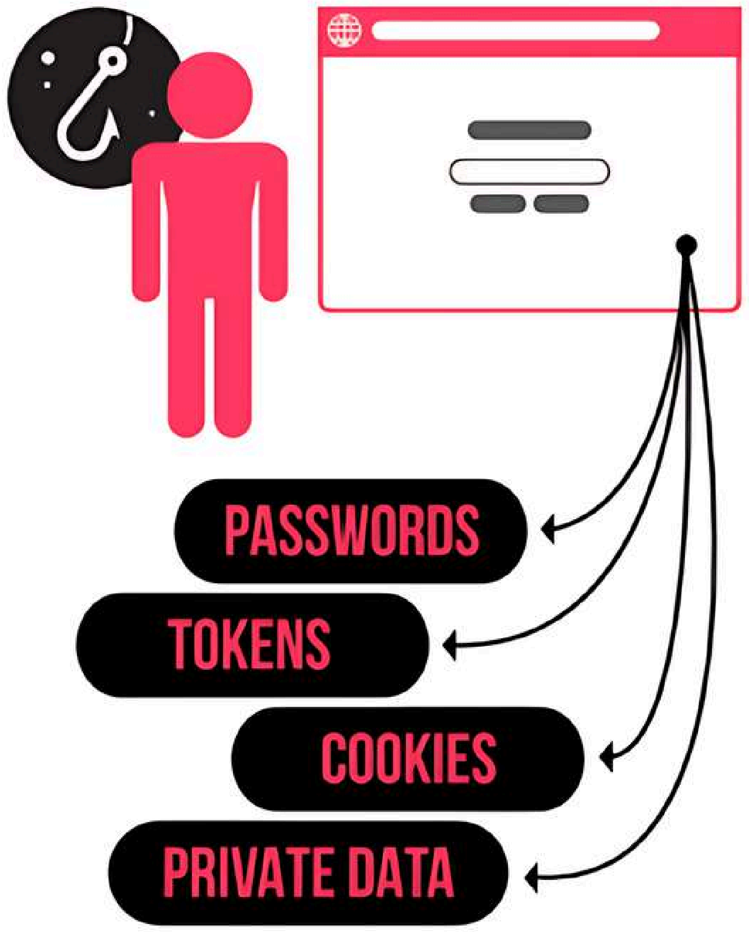
Total passwords cracked: 51

Passwords were cracked on computers within the environment. Hackers use tools like memory abuse, abusing user privilege, and ripping to obtain access to your passwords when you are phished. When this happens, these passwords are used to break into systems inside and even outside of the victim's environment. Below is a small sample of the passwords that were cracked. For a complete listing of passwords our team cracked by abusing user privilege refer to the detailed report.



COMPUTER NAME	BROWSER	LOGIN NAME	PASSWORD	URL
[redacted]	ChrEdge	[redacted]	[redacted]	https://www.clover.com/claim
[redacted]	ChrEdge	[redacted]	[redacted]	https://www.primepoint.net/eX/
[redacted]	Chrome	[redacted]	[redacted]	https://bergenrestore.vonigo.com/Securit...
[redacted]	Chrome	[redacted]	[redacted]	https://login.microsoftonline.com/common...
[redacted]	ChrEdge	[redacted]	[redacted]	https://auth.services.adobe.com/en_US/de...

Remediation: Work with users and train them to never store their passwords inside browsers or other memory on the device. Review the passwords that were uncovered during this evaluation, consider additional training around password complexity. Implement password manager with multifactor authentication capabilities to make it difficult for the attacker to get to the memory storing the password set. In addition, consider implementing web browser policies to enforce private browsing.

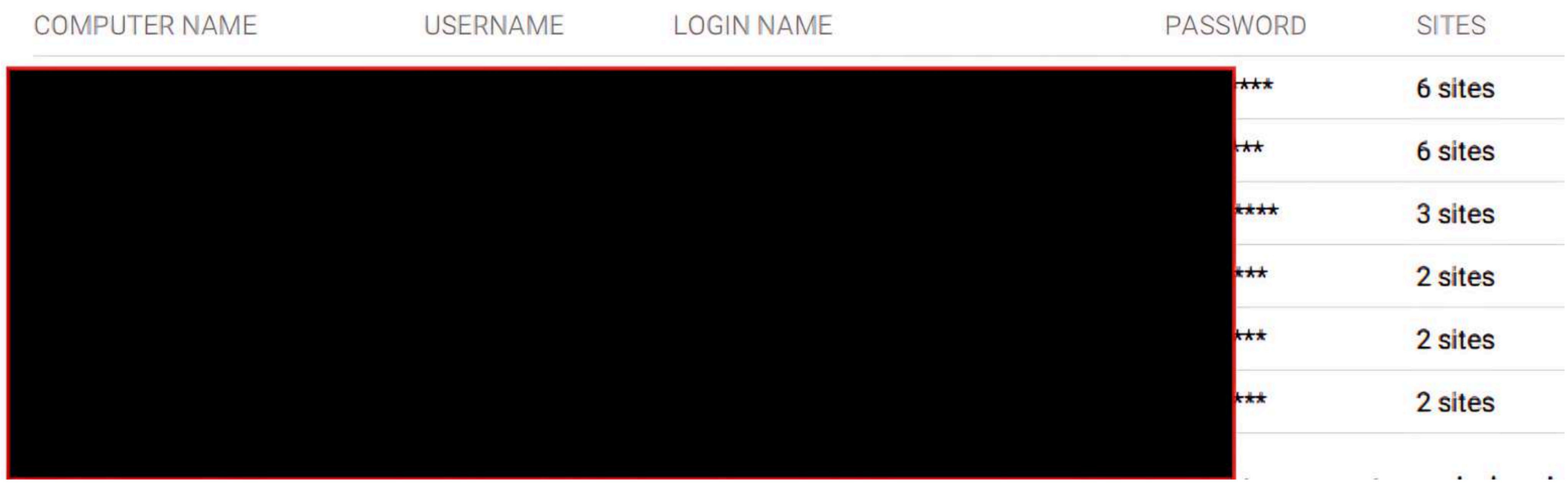


When a user is phished and clicks a link, there is one thing running EVERY SINGLE TIME: their web browser. Hackers quickly abuse the user's privileges, identify the cypher for the browser, and then use that cypher to access all passwords, tokens, cookies, and private data that web browser has access to. The attacker takes this data set and uses it to access additional accounts to find out more about their victim or to identify a list of people who trust the victim. They use this list to then infect other unsuspecting organizations.

ACCOUNTS HIGH RISK ISSUES

PASSWORD REUSE DETECTED - SUMMARY

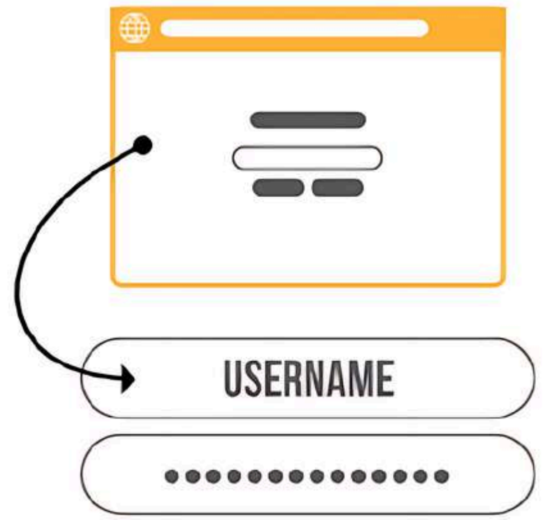
The same password appears to be used for multiple accounts or multiple cloud services. Attackers are constantly trying to break into networks using passwords they harvest by breaching external sites and cloud services. Because of this, reusing passwords in this way increases your risk for identity theft, spear phishing, and data breach.



COMPUTER NAME	USERNAME	LOGIN NAME	PASSWORD	SITES
[redacted]	[redacted]	[redacted]	[redacted]	6 sites
[redacted]	[redacted]	[redacted]	[redacted]	6 sites
[redacted]	[redacted]	[redacted]	[redacted]	3 sites
[redacted]	[redacted]	[redacted]	[redacted]	2 sites
[redacted]	[redacted]	[redacted]	[redacted]	2 sites
[redacted]	[redacted]	[redacted]	[redacted]	2 sites

Remediation: On average each user in a typical organization accesses 30 different accounts and cloud services. Consider a password manager to help your team manage all these passwords while avoiding password reuse. Based on these findings we also recommend training your team on managing proper methods for creating passwords.

OVER
300 BILLION
COMPROMISED PASSWORDS ARE AVAILABLE ON THE DARK WEB

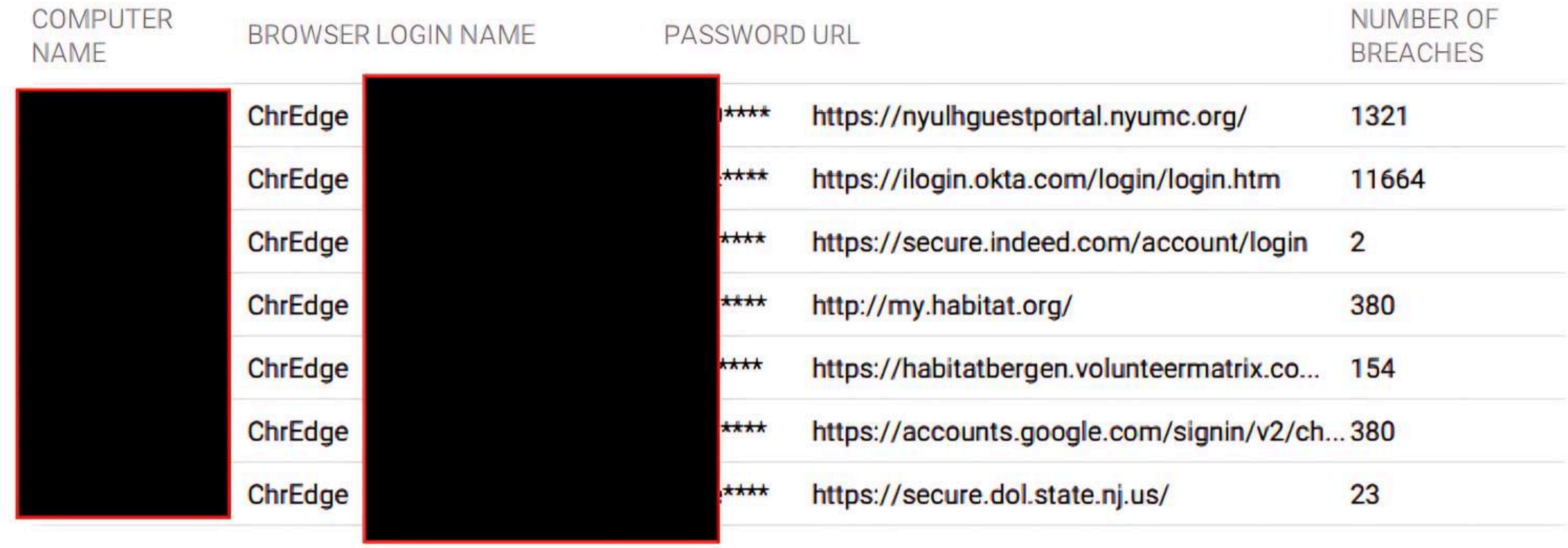


With over 300,000,000,000 compromised passwords available on the dark web, it is obvious that hackers know how to get their hands on passwords. How do they do this? One way is to steal them from websites. Breaches like Dunkin Donuts, Netflix, Gmail, Yahoo, Facebook, and LinkedIn produced billions of active username/password combinations. Currently hackers are crawling the internet using these passwords to try to get into networks like yours.

ACCOUNTS HIGH RISK ISSUES

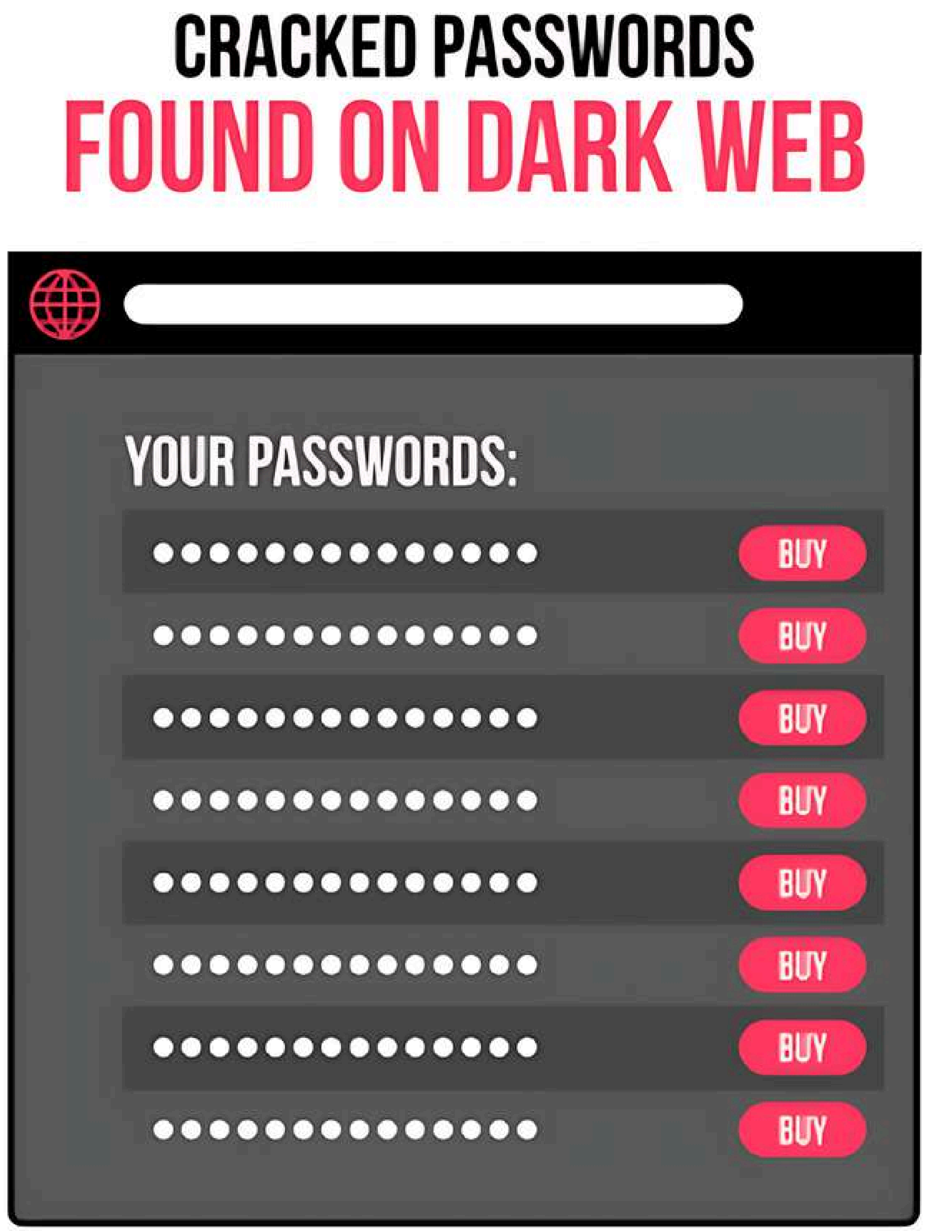
CRACKED PASSWORDS FOUND ON THE DARK WEB

Our team was able to crack a number of passwords. The passwords identified here should be addressed immediately. We were able to locate these within lists of passwords that are currently being shared on the dark web. This means that any account using this password may already be compromised.



COMPUTER NAME	BROWSER LOGIN NAME	PASSWORD URL	NUMBER OF BREACHES
[redacted]	ChrEdge [redacted]	**** https://nyulhguestportal.nyumc.org/	1321
	ChrEdge	**** https://ilogin.okta.com/login/login.htm	11664
	ChrEdge	**** https://secure.indeed.com/account/login	2
	ChrEdge	**** http://my.habitat.org/	380
	ChrEdge	**** https://habitatbergen.volunteermatrix.co...	154
	ChrEdge	**** https://accounts.google.com/signin/v2/ch...	380
	ChrEdge	**** https://secure.dol.state.nj.us/	23

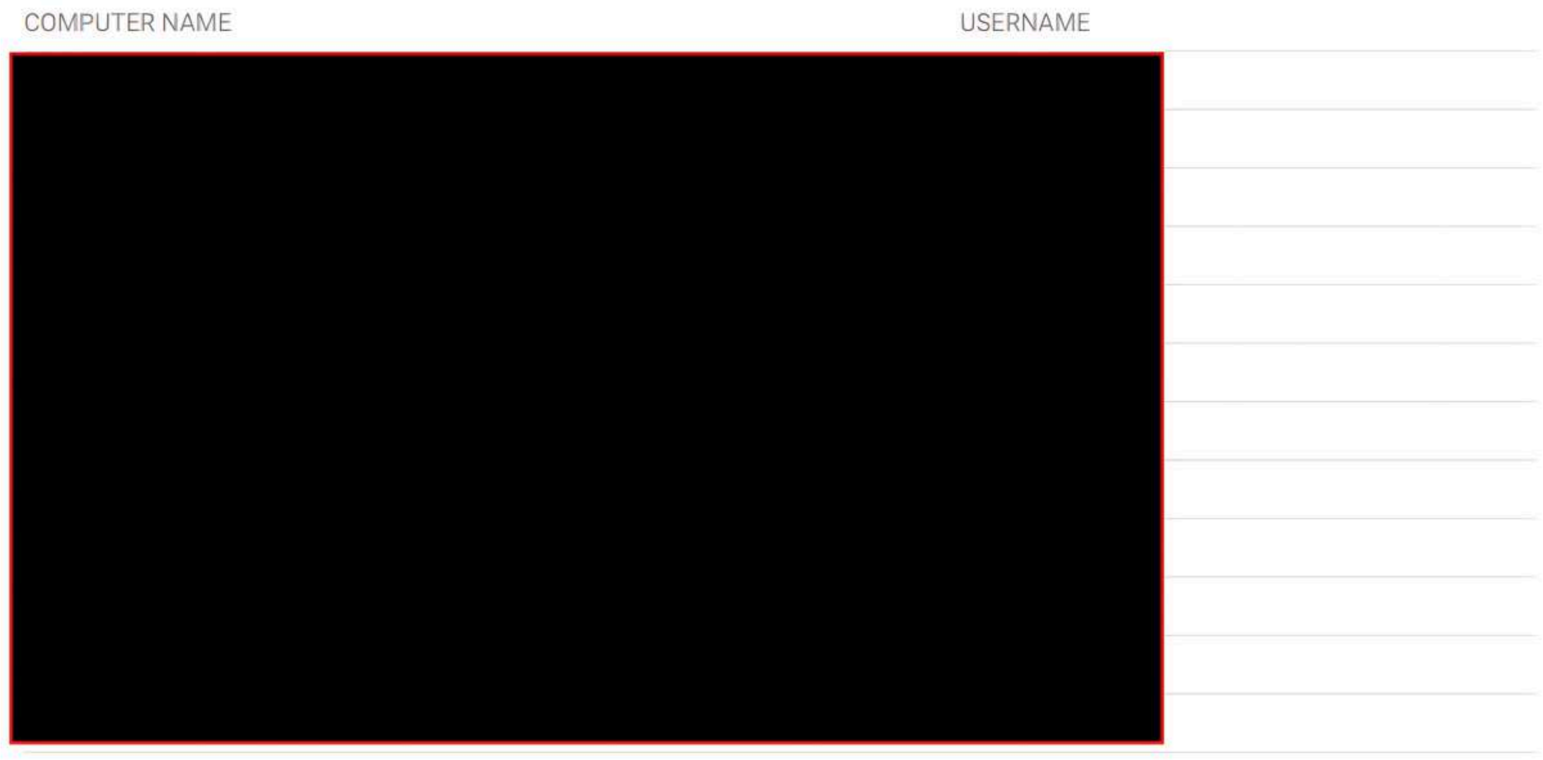
Remediation: Change these passwords immediately and look for indicators of compromise. A few indicators of compromise include logins from locations you do not expect, a large uptick in spam or phishing, or changes to your password you didn't make. Do not use these passwords again as they are already compromised



ACCOUNTS MEDIUM RISK ISSUES

ACTIVE USERS WITHOUT EXPIRING PASSWORDS

Attackers exploit leaked passwords to gain network access. Stale passwords jeopardize the network to breaches and attacks, and are completely preventable through an enforced password change policy.



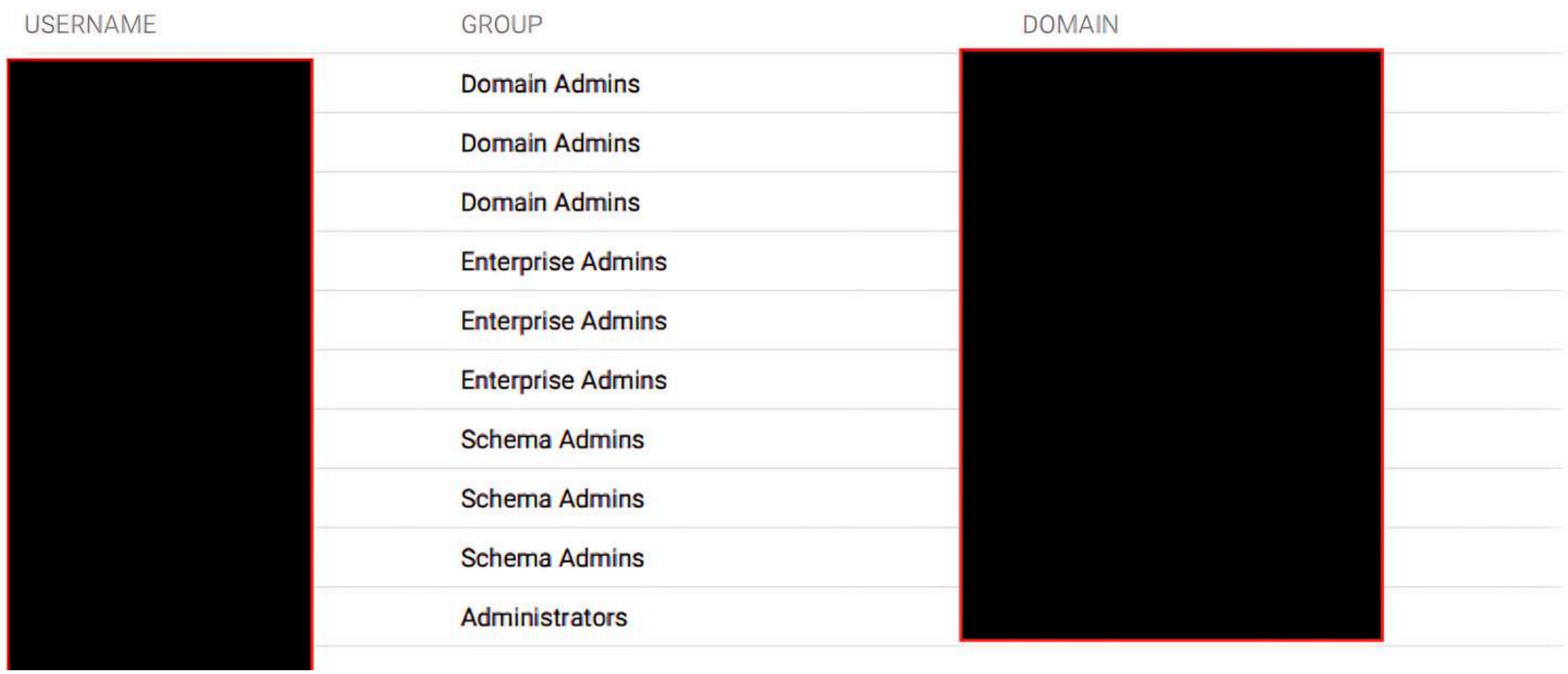
COMPUTER NAME	USERNAME
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Remediation: Enforce a password policy for all organization-related accounts. Monitor for non-compliance and remediate user password hygiene when necessary.

ACCOUNTS MEDIUM RISK ISSUES

ADMIN USER PASSWORD DOES NOT EXPIRE

Administrative user accounts have unrestricted access to critical infrastructure on the network. Hackers aggressively hunt for administrative credentials as a means to access your network. Stale administrator passwords open organization-wide risk to data breaches and attacks.



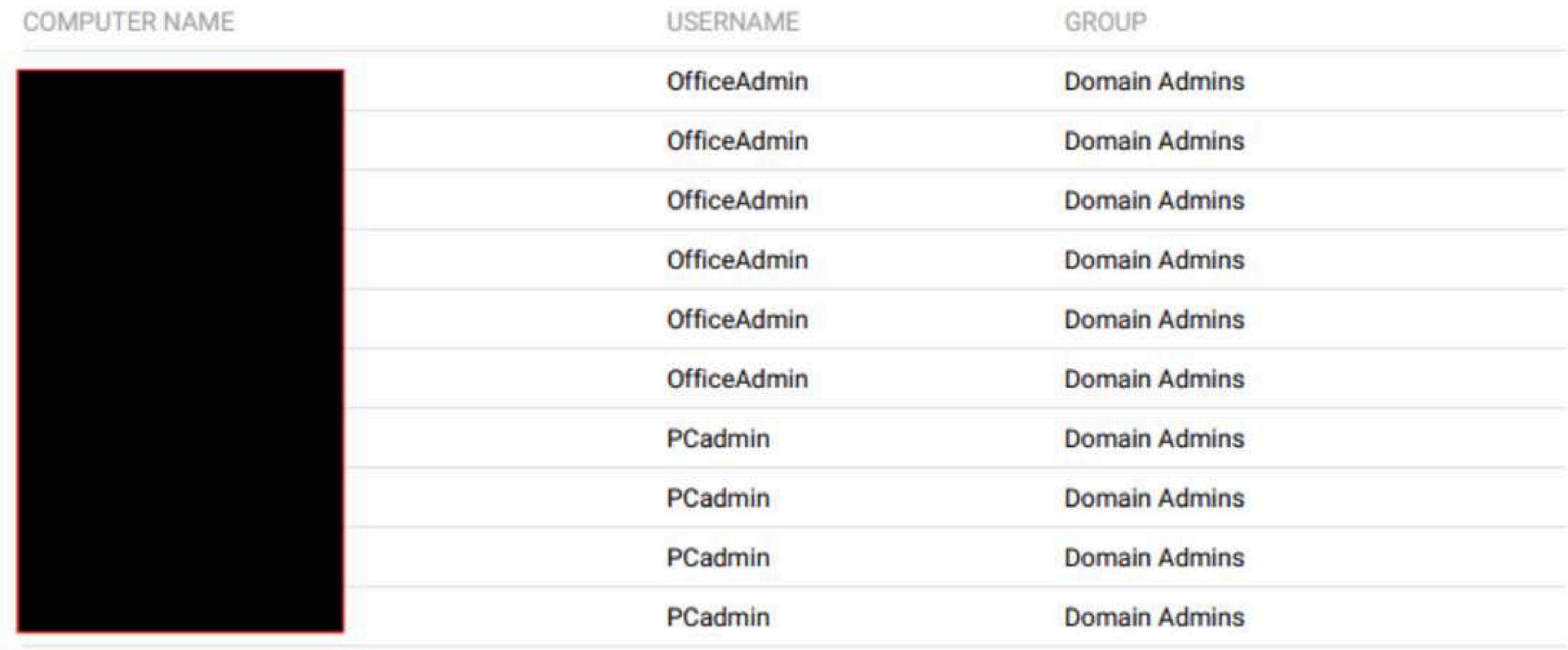
USERNAME	GROUP	DOMAIN
[redacted]	Domain Admins	[redacted]
[redacted]	Domain Admins	[redacted]
[redacted]	Domain Admins	[redacted]
[redacted]	Enterprise Admins	[redacted]
[redacted]	Enterprise Admins	[redacted]
[redacted]	Enterprise Admins	[redacted]
[redacted]	Schema Admins	[redacted]
[redacted]	Schema Admins	[redacted]
[redacted]	Schema Admins	[redacted]
[redacted]	Administrators	[redacted]

Remediation: Create a policy in Active Directory to force Administrative users to change their passwords periodically. Also consider enforcing password complexity, length, and reuse rules. Also, create guidelines when use of an Administrative account is acceptable.

ACCOUNTS

LIST OF IDENTIFIED DOMAIN ADMIN ACCOUNTS

We identified multiple accounts with Domain Admin rights on the network. Often accounts with administrative rights are provided to users that do not need this level of permissions. Having these accounts can put your organization at risk for an attack - especially if those accounts are being used for day-to-day use, as service, or default accounts.



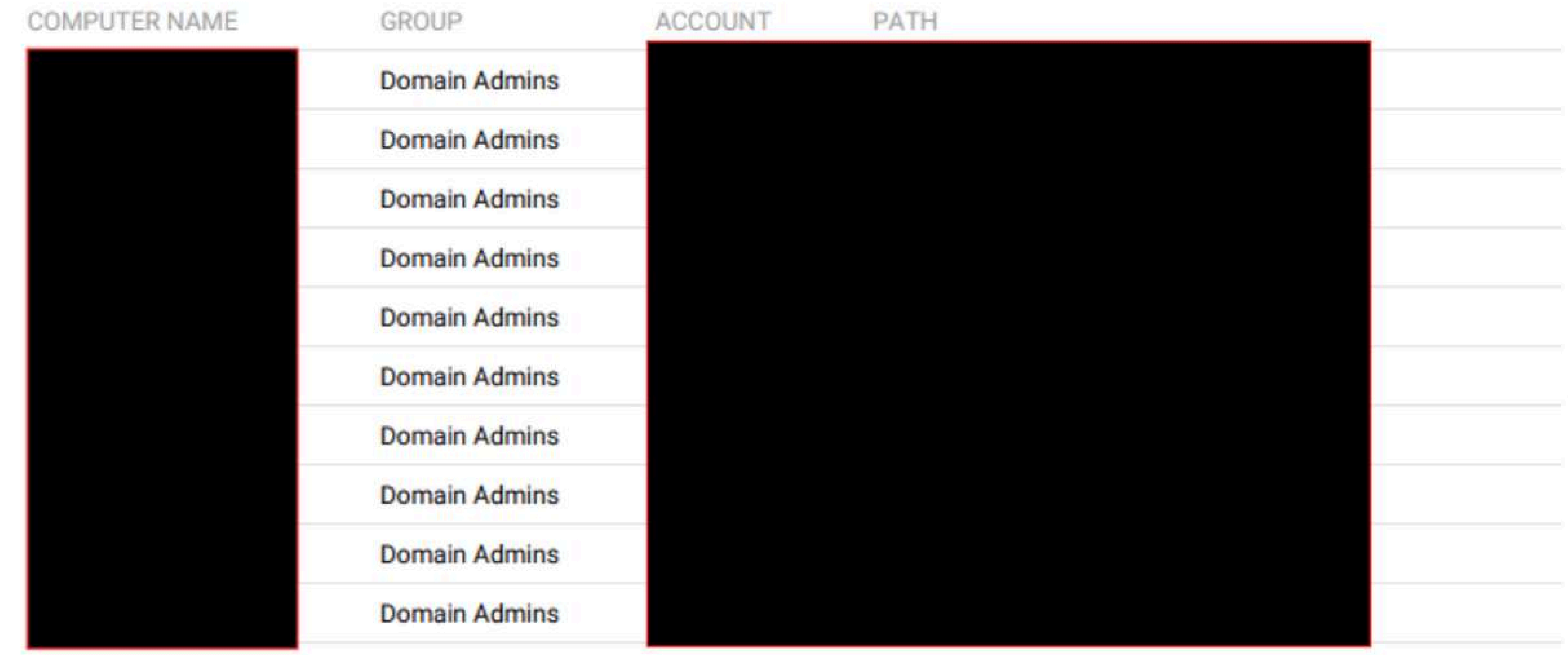
COMPUTER NAME	USERNAME	GROUP
[redacted]	OfficeAdmin	Domain Admins
[redacted]	OfficeAdmin	Domain Admins
[redacted]	OfficeAdmin	Domain Admins
[redacted]	OfficeAdmin	Domain Admins
[redacted]	OfficeAdmin	Domain Admins
[redacted]	OfficeAdmin	Domain Admins
[redacted]	PCadmin	Domain Admins
[redacted]	PCadmin	Domain Admins
[redacted]	PCadmin	Domain Admins
[redacted]	PCadmin	Domain Admins

Remediation: Review Domain Admin accounts and verify each user in the list should have these rights. Make sure these are not accounts that are used for day-to-day login and daily work.

ACCOUNTS HIGH RISK ISSUES

DOMAIN ADMIN CREDENTIALS FOUND CACHED ON MACHINE(S)

We found domain admin credentials cached/stored on at least one machine. Domain Admin account credentials are the keys to the kingdom. When domain admin passwords are cached, they can be easily hacked, opening up a hole to your entire network.



COMPUTER NAME	GROUP	ACCOUNT	PATH
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]
[redacted]	Domain Admins	[redacted]	[redacted]

Remediation: Turn off domain credential caching in the workstations, laptops, or member servers on which you might use Domain Admin credentials.

M365

USER ACCOUNTS NOT PROTECTED BY MULTIFACTOR AUTHENTICATION

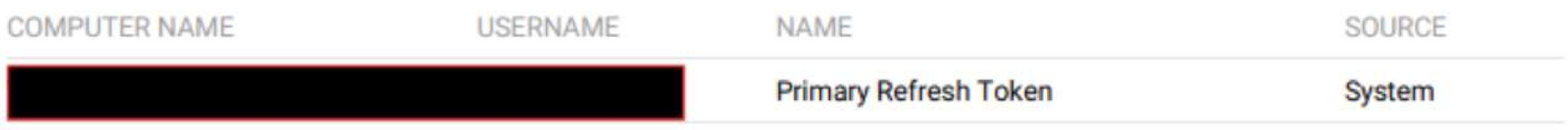
Multifactor Authentication (MFA) provides a critical additional layer of security by requiring users to verify their identity using some method that supplements their username and password alone - such as a numeric code sent to their smartphone via text or a specialized authentication app. By requiring this combination of “something you know” with “something you own,” MFA makes it much more difficult for attackers to maliciously impersonate legitimate users. (Note: This finding resulted from information obtained through personal interview.)

Remediation: Enable MFA on all M365 user accounts so that it can be implemented wherever and whenever it is appropriate to do so.

M365 HIGH RISK ISSUES

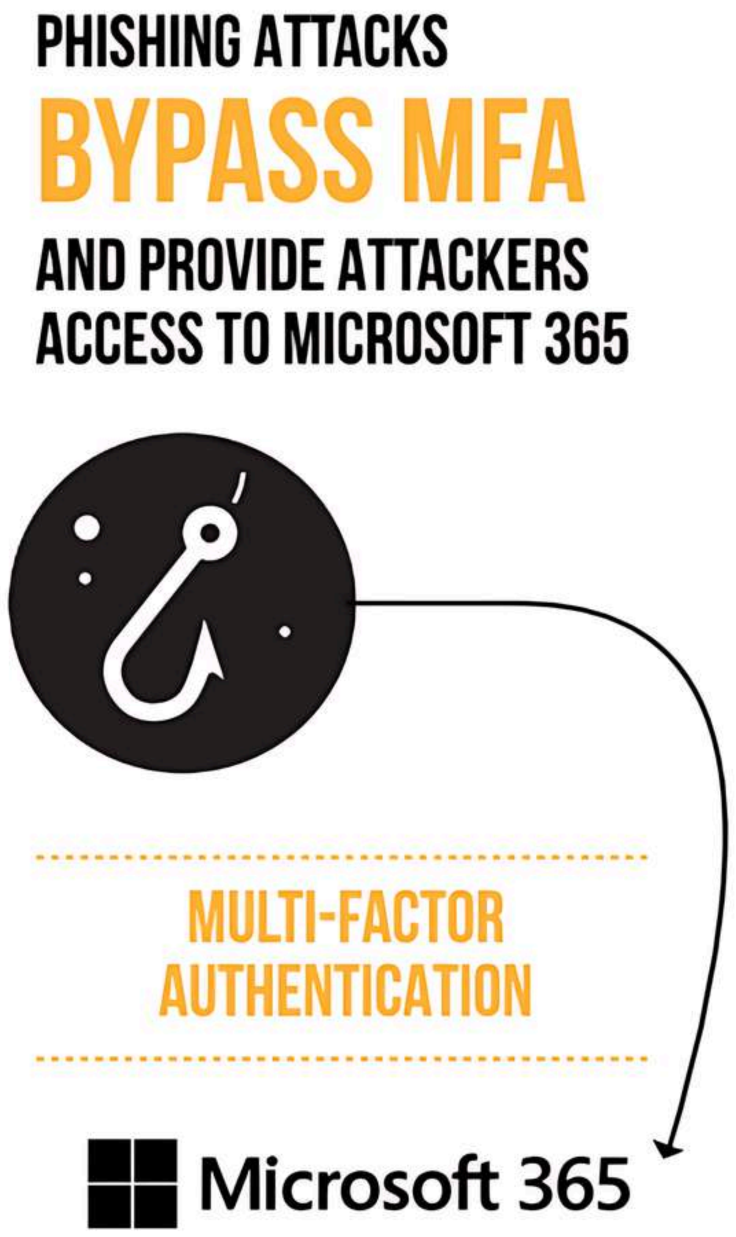
M365 SESSION TOKEN STOLEN

Hackers abuse memory and user privileges to access browser cookies and tokens. Cookies and tokens are the digital keys that allow users to have continued access to tools like M365 without having to re-enter their passwords. These may be keys that do not expire that our team was able to filtrate M365 for the users in this list. These are all keys that do not expire, giving the attacker access to each account until the user changes their password.



COMPUTER NAME	USERNAME	NAME	SOURCE
[redacted]	[redacted]	Primary Refresh Token	System

Remediation: Consider implementing secondary technical measures to minimize the danger of stolen M365 session tokens. These tokens are especially dangerous because they are usable even after the user logs off from their session. Always use private browsing to reduce the risk of stolen token cookies for privileged accounts like global administrator accounts.


PHISHING ATTACKS BYPASS MFA AND PROVIDE ATTACKERS ACCESS TO MICROSOFT 365

PATCHES

REMOTE ACCESS SOFTWARE DETECTED

Remote access software detected

COMPUTER	REMOTE ACCESS SOFTWARE
[redacted]	[redacted]

Remediation: Make sure that this remote access software is up to date or uninstall it if it should not be present.

PATCHES HIGH RISK ISSUES

MISSING WINDOWS SECURITY PATCHES

The following windows machines have vulnerabilities due to missing security patches.

COMPUTER NAME	CAPTION
[redacted]	

Remediation: Patch the machines to the latest available security patch.

PATCHES MEDIUM RISK ISSUES

POSSIBLE MISSING SECURITY PATCHES

The following windows machines have vulnerabilities due to missing non-windows. security patches.

COMPUTER NAME	CAPTION
[redacted]	

Remediation: Patch the machines to the latest available security patch.

ANTIVIRUS HIGH RISK ISSUES

SYSTEM DID NOT PRODUCE ALERTS FOR PASSWORD CRACKING ATTEMPTS

When an attacker phishes a user, they use tools on the device to crack passwords. It does not appear that the logs in this environment are producing the proper alerts for this type of behavior.

Remediation: Verify Windows Advanced Auditing is configured to detect malicious behavior like NTLM hash dumping.

EDUCATION

SYSTEM DID NOT PRODUCE ALERTS FOR PASSWORD CRACKING ATTEMPTS

Most attacks start with the user. According to a 2019 security report, 91% of cyber attacks start with a phishing email. Training can be the difference between a hacker getting your data and just getting past your technical defenses.

Remediation: Consider simulated phishing training to help users recognize phishing. Provide password management training and training on how to respond to a potential breach.

EDUCATION

SENSITIVE DATA BEING EMAILED

Our team added this finding due to an answer found on your questionnaire.
Sensitive data is allowed to be transferred through unsecure avenues like email.

Remediation: Since email is a highly unsecure way of sending PII (personally identifiable information) such as health related information or medical records, Social Security numbers, credit card, banking or financial information, it's essential to have emails encrypted to prevent the contents from being read by anyone other than the intended recipients. We strongly encourage a more extensive and robust assessment be done immediately to determine what, if any, exposure you may have.

EDUCATION

SENSITIVE DATA BEING SENT VIA CLOUD FILE-SHARING APPLICATIONS

Our team added this finding due to an answer found on your questionnaire.
Sensitive data is allowed to be transferred through cloud file-sharing applications.

Remediation: Depending on the type of file-sharing application used, you may have security considerations to address. We do not endorse the use of free versions of file-sharing applications. If file-sharing applications are in use, best practice is to use a business version that offers appropriate security controls to safeguard your data. Our assessment will detect if any file-sharing applications are installed on computers connected to your network. If file-sharing applications are found, we recommend a further analysis to determine if anyone is using the free versus business versions of these applications and if the data is being placed in these systems is being done so according to best practices to ensure the security of your data.

EDUCATION

NO CYBER LIABILITY INSURANCE IS IN PLACE.

Our team added this finding due to an answer found on your questionnaire.
No cyber liability insurance is in place.

Remediation: If your organization, handles stores, or has access to highly sensitive data (such as medical records), or any data that is required by law to be secured, we strongly recommend meeting with a qualified insurance professional who specializes in cyber liability to discuss getting a policy in place to cover financial losses that result from data breaches and other cyber-events. One single cyber-attack and quickly escalate making your office “ground zero” for attacks and data breaches for your clients. We also recommend reviewing policies regularly, in conjunction with performing risk and vulnerability assessments, to ensure the coverages align with your risk tolerance, and to ensure you are properly covered.

EDUCATION

CRIME INSURANCE IS IN PLACE

Our team added this finding due to an answer found on your questionnaire.
Crime insurance is in place.

Remediation: Good! As you know, a commercial crime policy provides coverage for a host of financial losses incurred from several crime related instances, such as vendor or employee theft, computer fraud, funds transfer fraud, ransomware and extortion, all of which are tactics commonly used by cybercrime rings. Make sure you contact your insurance professional to review your policy and ensure all of this is covered.

EDUCATION

WHERE DO YOU STORE YOUR LIST OF USER CREDENTIALS (USERNAME AND PASSWORDS) FOR YOUR EMPLOYEES?

Our team added this finding due to an answer found on your questionnaire.
Where the list of user credentials are stored.

Remediation: We strongly recommend against maintaining any list of usernames and passwords because documentation of usernames and passwords, particularly in one place or document, create a serious and significant security risk. Every user account should be unique and known only to the user. If you are maintaining these lists, we will help you implement a more secure credential management program.

EDUCATION

NO LISTED IT POLICIES ARE IN PLACE

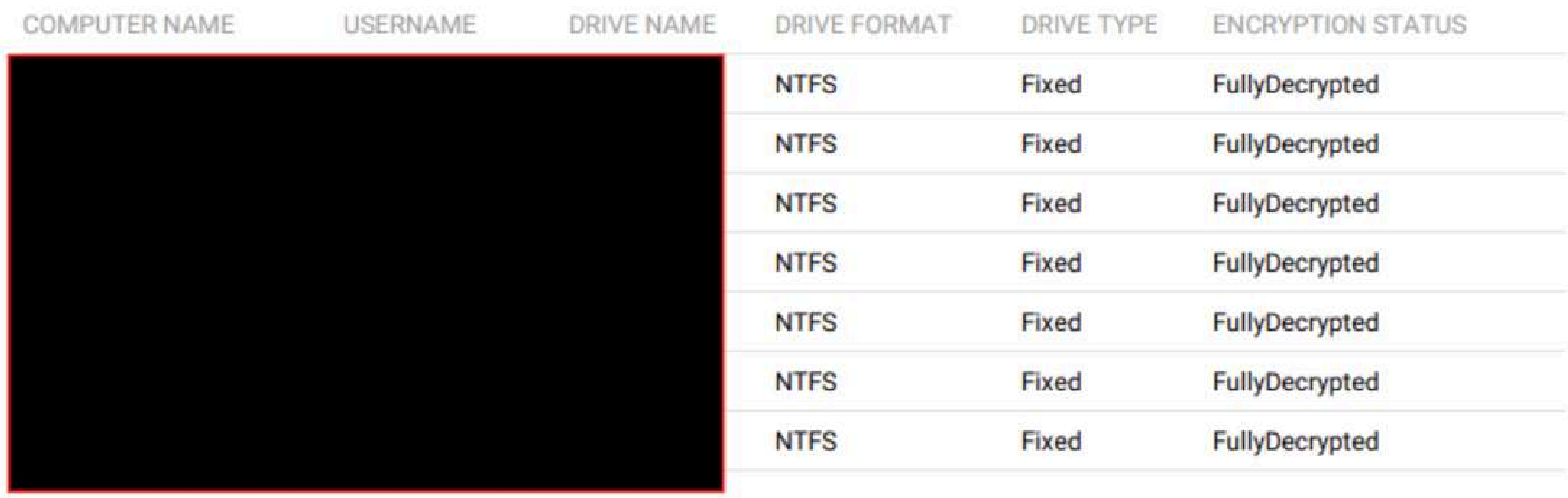
Our team added this finding due to an answer found on your questionnaire.
No listed IT policies were checked.

Remediation: If you want to protect your organization from cybercrime and demonstrate you are making a "best effort" to protect your clients’ and employees’ sensitive data, it is very important to have all the above policies and procedures in place. You must also have every employee sign off on your policies to confirm they have read, understand, and agree to comply with them. The signed policy should be scanned and maintained as part of the employees personnel file.

ENCRYPTION HIGH RISK ISSUES

UNENCRYPTED HARD DRIVES

The following lists all unencrypted drives found in the network.



COMPUTER NAME	USERNAME	DRIVE NAME	DRIVE FORMAT	DRIVE TYPE	ENCRYPTION STATUS
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted
[redacted]	[redacted]	[redacted]	NTFS	Fixed	FullyDecrypted

Remediation: Make sure drives are encrypted.

SURVEILLANCE MEDIUM RISK ISSUES

GENERAL SURVEILLANCE WARNING

See antivirus and firewall section - it does not appear that alerting is properly configured to detect an advanced persistent threat in the environment.

Remediation: See antivirus and firewall section to address issues.