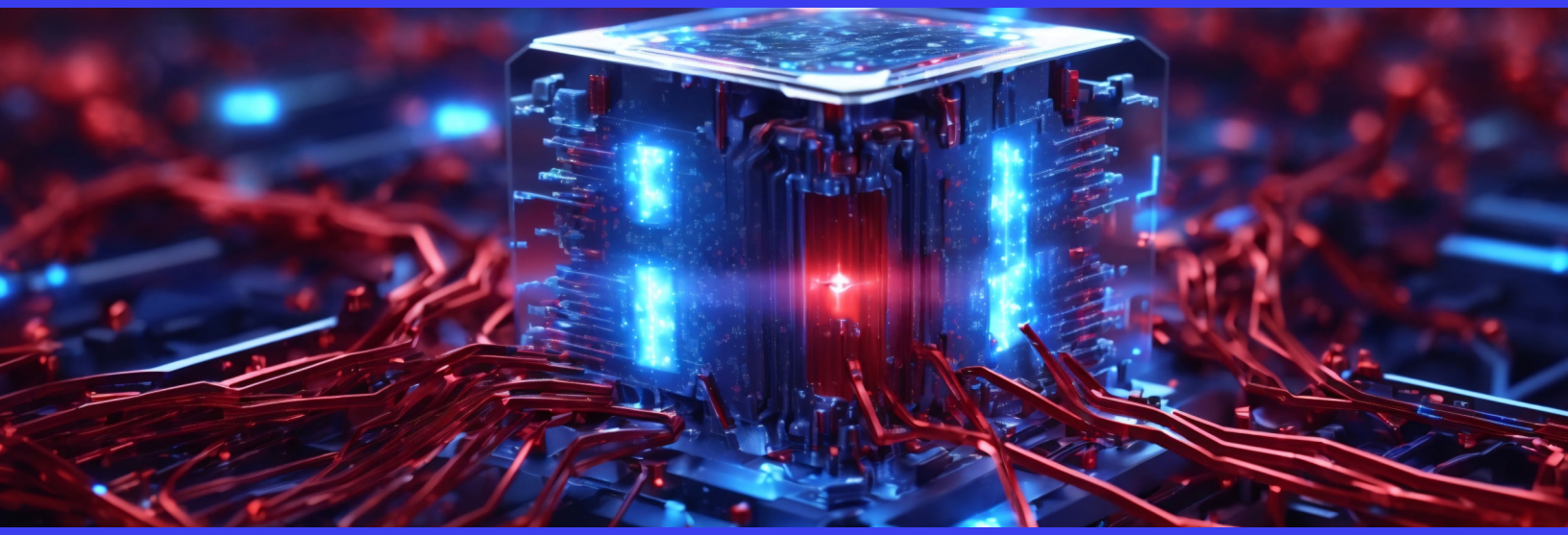
CONVERGE
TECHNOLOGY SOLUTIONS

PenTesting

A Red Team Review 2024

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 866.910.4425

Contents



INTRODUCTION

Shielding infrastructure, networks, and digital assets fuels the cybersecurity industry–a market likely to exceed **$208+ billion dollars globally** by the end of 2024.[1] Yet, what lies beneath the surface of every cybersecurity technology, service, or process is the intention of protecting people.

Company, organization, business, entity–regardless of which term you use, there is a mosaic of people who power its systems. Securing these individuals is essential to securing the systems.

Even as a legion of cybersecurity tools and processes are developed and improved to protect a widening attack surface, cybersecurity still comes down to the intricate interplay of human behavior and decision-making.

Protecting the individual is necessary for protecting the organization. It's a symbiotic relationship and our analysis shows that human factors are the pivotal elements standing between an enterprise and its cyber attackers.

METHODOLOGY

This report is an analysis of the combined penetration testing results of Converge's 30+ penetration testers. As part of our Advanced Testing practice, our red team blends the ingenuity of a hacker mindset with a white-hat passion to outwit attackers and protect people.

200
Penetration Tests

30,000
Assets

150+
Unique Clients

28+
Industries

1. MarketsandMarkets, Global Cybersecurity Industry Outlook 2024, Web, https://www.marketsandmarkets.com/Market-Reports/cyber-security-industry-outlook-217338166.html

EXECUTIVE SUMMARY

The most critical security challenges facing organizations are balanced on the fulcrum of credentials. As more attacks leverage credentials to widen security gaps for access, it is now an absolute imperative for organizations to use all tools available to protect them.

Analyzing the data of the top 10 attack techniques our testers abused show that the top six related to passwords. Three enabled the capture and relay of credentials due to operating system misconfigurations, including one vulnerability that we identified as the most common vulnerability throughout 2023. Rounding out this top 10 list is poor application development practices that led to exploitable vulnerabilities in custom applications. The results are neither a surprise nor a new development.

Top Test Cases

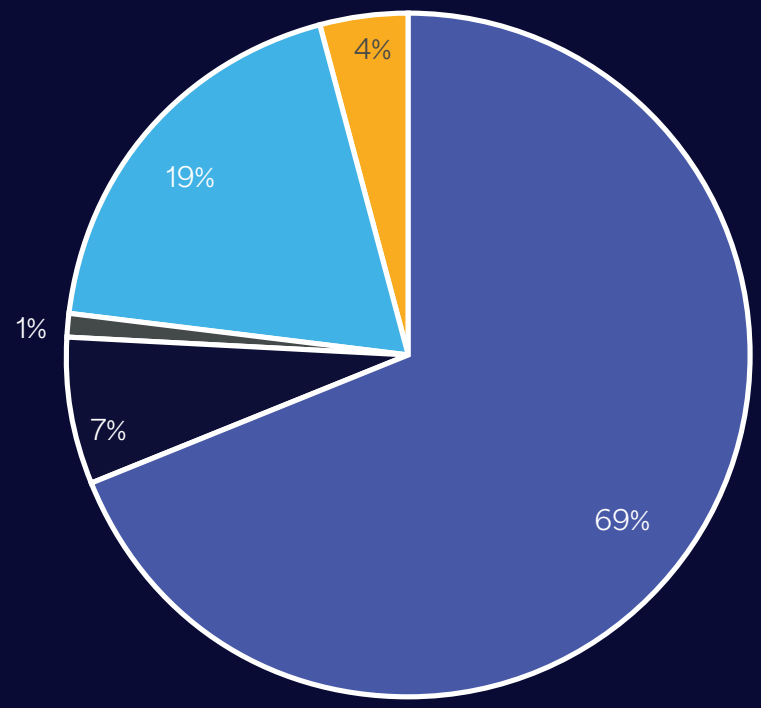
Converge penetration testers found the most success in abusing these test cases to further their objectives.

1. Credential relay attacks
2. Reuse of local administrator credentials
3. Abuse of default Windows legacy network protocols that enable poisoning and credential theft
4. Kerberoasting
5. Use of default credentials
6. Insecure or incorrect implementation of IPv6 traffic routing that enables poisoning and credential theft
7. Use of weak or predictable passwords
8. Reuse of non-privileged credentials
9. Presence of default accounts
10. Web application exploitation

Key Vulnerability Statistics

Top 10 Exploitable Vulnerabilities

1. SMB Signing Not Required
2. Local Administrator Credential Reuse
3. LDAP Signing & Channel Binding Not Required
4. Default Credentials
5. Kerberoasting
6. Cisco Smart Install Use
7. Multicast Name Resolution Poisoning
8. Microsoft RDP RCE
9. MS17-010 EternalBlue
10. Passwords Stored in Active Directory User Account Description Field



NOTABLE TRENDS

One of the emerging trends stood out in our data. Misconfigurations in Active Directory Certificate Services (ADCS) were abused more frequently to escalate access from a low-privileged account to domain administrator access, often using the credential-based and adversary-in-the-middle attack techniques illustrated above.

Organizations use ADCS to generate their own certificates, usually for internal applications, VPN authentication, smart cards, or similar contexts. Our team was able to routinely abuse misconfigurations in certificate templates using a previously compromised standard account to request a certificate for any account, including domain administrators. This technique can be used in an attack chain that allows an attacker to authenticate as a domain administrator.

Many other privilege escalation attacks were successful against insecure Active Directory permissions. We recommend that cybersecurity teams incorporate offensive tooling into their regular auditing practices. A variety of tools are available to assist with these functions; **we find the following useful**:

Attack Path Mapping: Bloodhound, PingCastle

ADCS Vulnerability Discovery: Certipy

Kerberos Configuration Risks: Impacket, Rubeus

These additional trends also standout and are likely to continue to grow.

Application attacks: Initial external compromise is increasingly facilitated through application-layer attacks in both commercial and custom developed applications.

MFA bypass: As organizations successfully transition more of their perimeter authentication controls to leverage multifactor authentication (MFA), attackers are pivoting to alternative attack paths. Phishing and password spraying have evolved, with attackers integrating the ability to sit transparently between victim browsers and backend authentication systems and phishing websites passing through authentication to compromise user sessions. Attackers are using MFA fatigue attacks to repeatedly log into an account, typically compromised via password spraying, to cause numerous MFA push notifications for the end user. Victims are often coerced into accepting a push approval to stop the onslaught of notifications.

Social engineering takes a turn

Phishing is underscored as a highly successful and enduring technique used by malicious adversaries. It's still in the cyber attacker toolkit, but we've seen a shift in the last 12 months, as non-phishing techniques go mainstream.

Security awareness training and strong security controls at the email perimeter have taken some of the shine off phishing campaigns. Attackers are noticing this lowering success rate, leaning more into vishing, a phone-based social engineering tactic, and smishing, which uses text messaging, to bypass corporate security controls. The attack on the MGM casino provided mainstream visibility into how these threats unfold.

Application security takes center stage

Review of our testing data shows that applications are vulnerable and targeted. New and continuing trends plague efforts to protect applications. The OWASP top 10 vulnerability classes are still common, but more severe types of vulnerabilities within these categories are surfacing.

The statistics show that a large portion of Converge's application testing identifies some form of injection attack, but that vulnerabilities that don't neatly fit into the **OWASP top 10 categories are a growing trend.**

OWASP Top 10 Correlation

A1	Broken Access Control	14%
A2	Cyrpotgraphic Failures	1%
A3	Injection	48%
A4	Insecure Design	<1%
A5	Security Misconfiguration	2%
A6	Vulnerable and Outdated Components	23%
A7	Identification and Authentication Failures	1%
A8	Software and Data Integrity Failures	<1%
A9	Security Logging and Monitoring Failures	<1%
A10	Server-Side Request Forgery	<1%
	Vulnerabilities Outside of Clear Alignment With OWASP Classifications	12%

New attacks are frequently chaining a mix of the common OWASP top classes of vulnerabilities with more complex issues. Among the more severe instances are: Mass parameter assignment and object clobbering; irregular forms of authentication bypasses leading to remote code execution; parameter tampering to escalate privileges; continuously changing SQL injection forms.

Our testers identified these critical vulnerabilities to bypass authentication, escalate privileges, and obtain remote code execution on multiple client engagements using custom scripts and tooling created to perform these attacks and exploit any unconventional bugs that were identified.

Diligent and creative application of adversarial tactics against some of these weaknesses were applied by one of our skilled testers, who discovered and responsibly disclosed a **9.8 critical vulnerability in the CrushFTP managed file transfer (MFT) application**.[2]

CVE-2023-43177
9.8 Critical
10,000+ Public Instances

Identified as CVE-2023-43177, this vulnerability impacted a known base of 10,000+ public instances and many more private networks. Our tester determined that exploitation of this vulnerability permitted an unauthenticated attacker to access all CrushFTP files, run arbitrary programs on the host server, and acquire full access to the underlying host.

The attack chain included:

- Abuse of a header parsing vulnerability in a lesser-known protocol called AS2
- Mass assignment vulnerability leading to overwriting of a key variable
- Arbitrary file read/write vulnerability for leaking session data and escalating privileges
- Arbitrary Java code execution

Our tester's discovery of this zero-day vulnerability gave Converge clients the advantage of early warning, allowing for the appropriate remediations to occur before the adversaries had a chance to move from detected proofs of concept to anticipated exploitation. The CrushFTP zero day joined other impactful MFT attacks in 2023 that saw attackers increasingly use the high availability of these applications for success as an initial attack vector.

Early in 2024, the **GoAnywhere and MoveIt Transfer MFT attacks**[3] were included on a list of the biggest zero-day attacks for 2023. The GoAnywhere attack made the top spot, likely based on the large web of impacted organizations, such as vendors like Rubrik and brand houses like Proctor & Gamble. The number three position was filled by the MoveIt Transfer vulnerability which leveraged a SQL injection flaw and lingered in the headlines for months as the list of impacted victims grew. Both MFT attacks had ties to the Clop ransomware gang.

2. Ryan Emmons and Evan Malamis, Converge Technology Solutions, (Nov. 16, 2023), Blog, https://convergetp.com/2023/11/16/crushftp-zero-day-cve-2023-43177-discovered/

3. Rob Wright, TechTarget, (Jan. 4, 2024), Web, https://www.techtarget.com/searchsecurity/feature/10-of-the-biggest-zero-day-attacks-of-2023

KEY TAKEAWAYS

Fewer security assumptions, more assurance

Fewer organizations are taking an overconfident view of their current security measures, and that's a good thing. It brings with it the realization that "don't fix it if it's not broke" doesn't work for security. When something fails in an organization's security posture, the impact can cost millions of dollars of lost revenue, reputation, and resources. You can stand still with your cybersecurity and let the attackers come to you (and they will), or you can proactively commit to maturing your organization's security.

The trend for more proactive maturity is observable within our client base, as we see more interest in on-going and recurring penetration testing. Our clients are reducing obvious, well-identified vulnerabilities, gaining better understanding and management of their attack surfaces, and accelerating remediation efforts more effectively because of improvements to cybersecurity programs.

Undeniable value of identity and access management

Attackers use a seemingly endless level of persistence and skill to gain access to credentials. So does our red team, successfully capitalizing on privileged account vulnerabilities time and again. Our exploitation of Active Directory Certificate Services (ADCS)–a core function of identity management–shared earlier in this report show that there are still significant gaps in this area. Organizations need to accelerate identity and access management (IAM) programs to address the gaps that malicious adversaries routinely abuse.

Tools that filter passwords based on known compromises, brand keywords, and other common password terms like months or seasons of the year, are affordable and tremendously effective at reducing the human tendencies of employees to select weak passwords. Privileged access management (PAM) tools help ensure that local accounts use unique, differentiated passwords and that privileged accounts are tightly controlled, reducing an attacker's ability to obtain and use privileged credentials. Using these tools provides a countermeasure against credential attacks, and can significantly reduce how long an attacker is able to use a compromised account.

Make the most of available vendor support, tools, and threat intelligence. In the case of the identified risk with ADCS, Microsoft strongly supports protections for Active Directory and its other systems and services to reduce the ability for unauthorized escalation of privileges. Several classes of attacks can be eliminated by implementing freely available guidance and tools to harden and secure Microsoft environments.

Evolving focus of social engineering threats

Adversaries are shifting their social engineering strategies with techniques that bypass MFA and leverage artificial intelligence and deepfakes. They are also shifting their focus on delivery–moving attacks to the phone, using vishing and smishing to coerce victims, and inserting QR codes into delivery messages.

Organizations must review their training programs to ensure that security awareness training adapts to the new attack vectors that are gaining popularity with attackers. Training programs should include the risks of vishing, as well as the growing trend of using artificial intelligence to create deepfakes to impersonate voices that can

coerce victims into providing the information attackers are after. Employees should be trained on the methods that can properly authenticate a caller. The risk of push notifications should be highlighted and training should help employees recognize that unprompted push notifications are signs of an attack. Disabling push notifications is ideal, with a more secure means of MFA enabled.

Top Three Things to Do Now

1. Enforce strong password policies and processes with additional identity and access management tools.
2. Assess and update existing security awareness training programs to provide training for and testing of vishing attacks, deepfakes, and more sophisticated techniques.
3. Expand application security programs into the CI/CD pipeline in conjunction with tooling that identifies and automatically alerts on vulnerabilities in software, configuration files, and build scripts.

OUTLOOK

Behind the curtain of application security

Organizations who have development functions should ensure that regular application penetration testing is combined with their tooling. The application attacks we are seeing include increasingly complex attack chains that abuse high-risk, high-impact vulnerabilities.

Converge's application penetration testing results demonstrate that older vulnerability classes persist, but newer and more complex chains of attacks are being identified regularly. Simply performing application-layer scanning and code reviews is not enough. Likewise, a single, annual penetration test is no longer sufficient.

The increasing complexity of application environments requires organizations to take a holistic approach that combines proper threat modeling and security requirement development in the planning stages for any new development project or any major change.

This should be combined with static application security testing built into the development pipeline, and both automated web application scanning and manual web application penetration testing should be performed by experts on a regular basis. Mature organizations should consider implementing runtime application self-protection (RASP) and application security posture management (ASPM) to further reduce the risk of application or data compromise.

20%-30%
Savings Over Single Tests

79 NPS
Client Satisfaction Score

100%
Human Tested & Validated

100%
US-Based Testers Employed by Converge

Know Sooner & Act Faster With Converge PTaaS

Our Penetration Testing as a Service (PTaaS) delivers the flexibility and pricing advantages you need to stay on top of developing vulnerabilities in dynamic environments. We connect the essential elements of deep, effective penetration testing with budget advantages to arm you with information that protects your organization in its current state.

- Certified, creative testers with an adversarial mind-set
- Near-real time progress tracking and reporting
- Advanced security tools
- Layered threat intelligence
- Custom dashboard
- Direct access to testers and project management
- Risk-ranked vulnerabilities
- Detailed remediation steps

Advanced Testing Services

Supercharge the exposure and exploitation of weaknesses in your environment.

Our penetration testing is people-powered and technology-driven for creative exploitation as advanced as real-world adversaries.

Delivered as Single Testing Engagements or With PTaaS

Application	Red & Purple Teaming
Cloud	Social Engineering
Network	

Top-Level Certifications

OSCP · OSEP · OSWA · OSWE · PNPT · GPEN · GWAPT

Converge Advanced Testing by the Numbers

19+ Years of Experience

200+ Penetration Tests Each Year

150+ Unique Clients Served Each Year

30+ Staff Resources

15 Top-Secret Clearance

AUTHOR

Josh Berry

Director of Advanced Testing & Governance, Risk & Compliance

josh.berry@convergetp.com

CONVERGE
TECHNOLOGY SOLUTIONS

convergetp.com/cybersecurity