PICNIC™

TARGET INTELLIGENCE REPORT | ISSUE NO.2

UBER

LESSONS LEARNED

Prepared by:
MANIT SAHIB & FELISHA MOUCHOUS
Office of Global Threat Intelligence, Picnic Corporation

getpicnic.com

TABLE OF CONTENTS

INTRODUCTION

Social engineers collect intelligence on human targets to develop paths for attack and compromise. Picnic's platform emulates this external, human attack surface reconnaissance to expose **TARGET INTELLIGENCE** about an organization. Picnic pairs this unique perspective of threat actors with automated actions that reduce risk for its customers.

Picnic offers Target Intelligence Reports to help security teams better understand how attackers use open-source intelligence and established infrastructure to launch attacks. By reducing their human attack surface, organizations can disrupt attacker reconnaissance and resource development, which in turn reduces the risk of attacks.

EXECUTIVE SUMMARY

In this report, we analyze **the Uber September 2022 data breach** to understand how the attacker leveraged open-source information and social engineering to target an Uber contractor. The report includes proactive remediation steps for organizations to take to help lower the risk of attackers being successful in the future.

We used Picnic's platform to expose threat actor reconnaissance and resource development. We also analyzed public reporting about the attack to provide a more complete picture of the attack and remediation actions taken by victims.

Overall, our findings highlight how important it is for companies to proactively understand, limit, and continuously monitor employee and organizational exposure, and to preemptively identify and block attacker infrastructure. Combining these capabilities can mitigate the threat of attackers launching successful social engineering attacks against organizations.

The data in this report is valid through April 2023.

UBER INCIDENT SUMMARY

September 2022

Uber is a US-based company that provides ride-hailing and food delivery services to consumers worldwide.

On September 15th, 2022, a hacker compromised Uber and released screenshots from internal Uber systems to reveal the hack. These included images from Uber's Slack, emails, other internal systems, HackerOne account, AWS, VMware, GCP, and SentinelOne instance. Employees from Uber are reported to have initially believed the posts were a hoax when they first appeared on the Slack channel.

On September 19th, 2022, Uber released a statement detailing more information about the attack. According to the statement, the actor appeared to have purchased an Uber corporate password on the dark web after a contractor's personal device was infected with malware. The hacker then used these credentials to log in repeatedly, which prompted an MFA login approval request. The hacker allegedly used WhatsApp to contact and encourage the contractor to click on the push notification.

After successfully exhausting the contractor with this MFA fatigue attack, the approval was granted, and this provided the hacker with the valid credentials needed to gain access to Uber's VPN.

Once inside, the hacker found a network share that had PowerShell scripts.

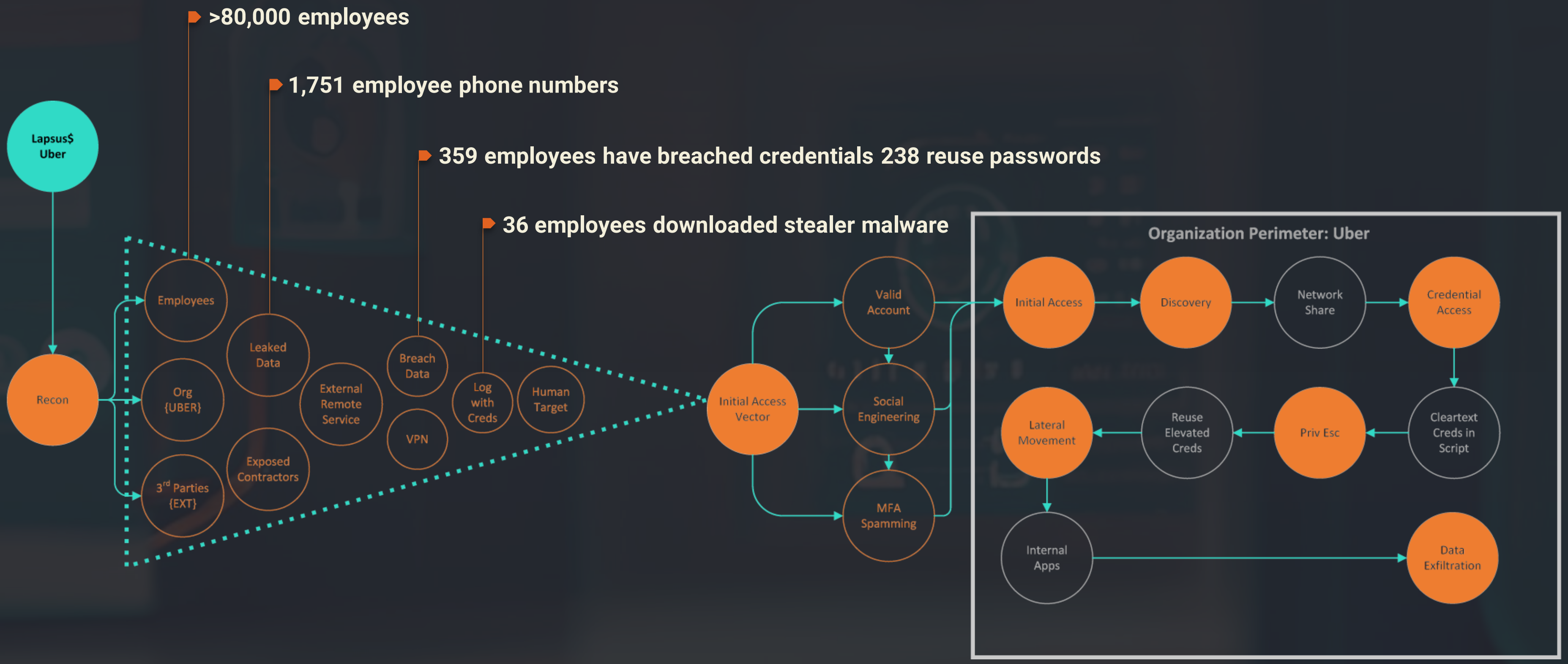
One of these scripts contained admin credentials for Thycotic, a privileged access management solution. Once the hacker had access to this, he was able to get access to all other internal systems by using their passwords.

Uber stated that no production systems or customer data were breached during this attack and no changes were made to the existing codebase. As of September 2022, Uber was working with a digital forensics firm and making security improvements internally. Uber concluded that the actor responsible was likely affiliated with the cybercriminal group Lapsus$, and also connected to the Rockstar Games hack which occurred around the same time.

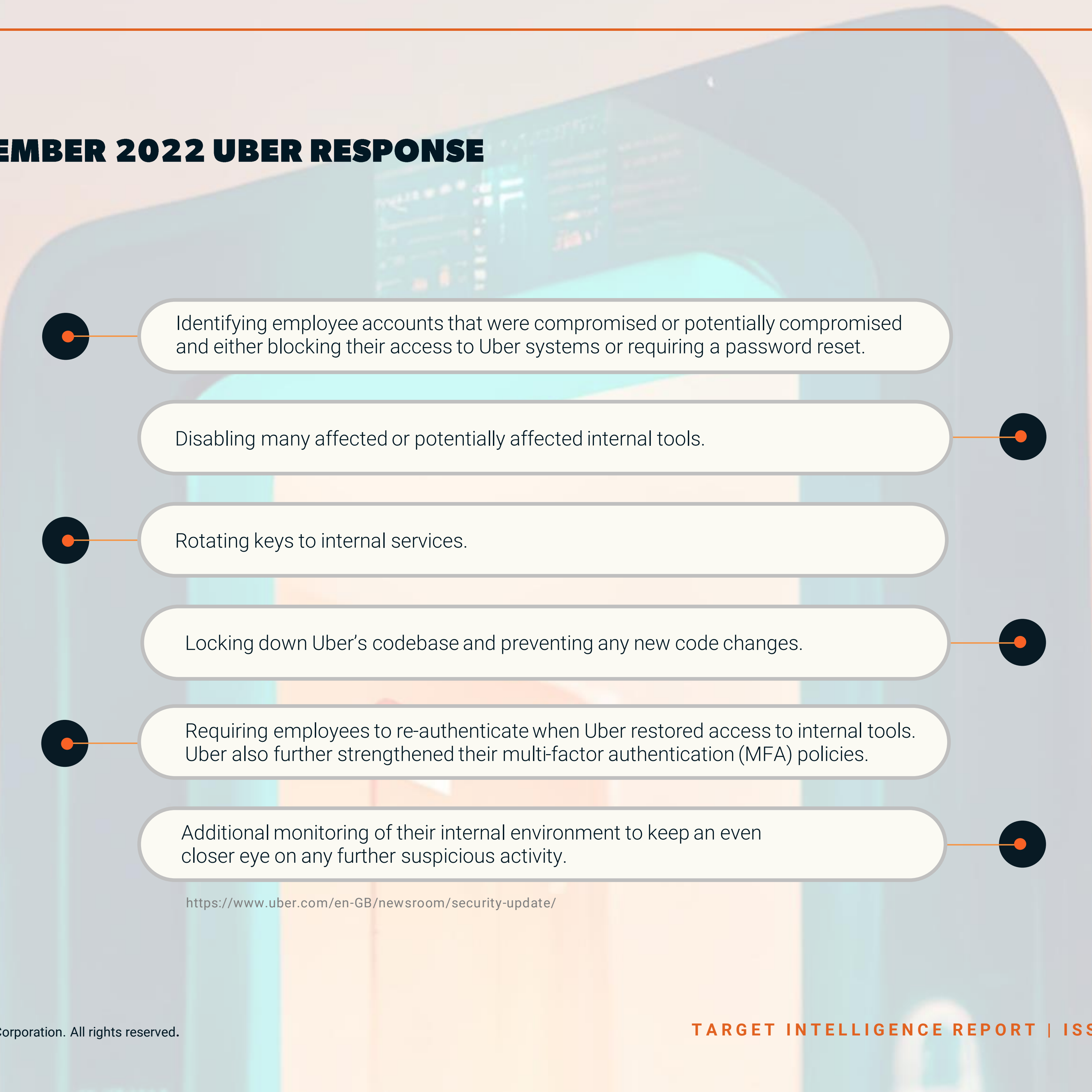
On September 22, 2022, the City of London Police arrested a 17-year-old male in Oxfordshire, England, who was charged with multiple counts of computer misuse and breach of bail. Although the police did not comment, it is highly likely that the male arrested was the same one arrested previously in March 2022, when his name was published online in connection with Lapsus$.

UBER INCIDENT SUMMARY CONT.

Lapsus$ September 2022 Uber Breach Compromise Path



SEPTEMBER 2022 UBER RESPONSE



- Identifying employee accounts that were compromised or potentially compromised and either blocking their access to Uber systems or requiring a password reset.
- Disabling many affected or potentially affected internal tools.
- Rotating keys to internal services.
- Locking down Uber’s codebase and preventing any new code changes.
- Requiring employees to re-authenticate when Uber restored access to internal tools. Uber also further strengthened their multi-factor authentication (MFA) policies.
- Additional monitoring of their internal environment to keep an even closer eye on any further suspicious activity.

https://www.uber.com/en-GB/newsroom/security-update/

THREAT ACTOR

Lapsus$

Lapsus$ aka DEV-0537 (Microsoft Designation) is known for using a pure extortion and destruction model without deploying ransomware payloads. DEV-0537 started targeting organizations in the United Kingdom and South America but expanded to global targets, including organizations in government, technology, telecom, media, retail, and healthcare sectors. Some companies that have fallen victim to this attacker include Okta, Microsoft, Vodafone, Nvidia, Rockstar Games, and Uber.

This group publishes its breaches via Telegram and is very vocal on this platform in order to promote its activities and cause reputational damage to the organizations it has managed to compromise.

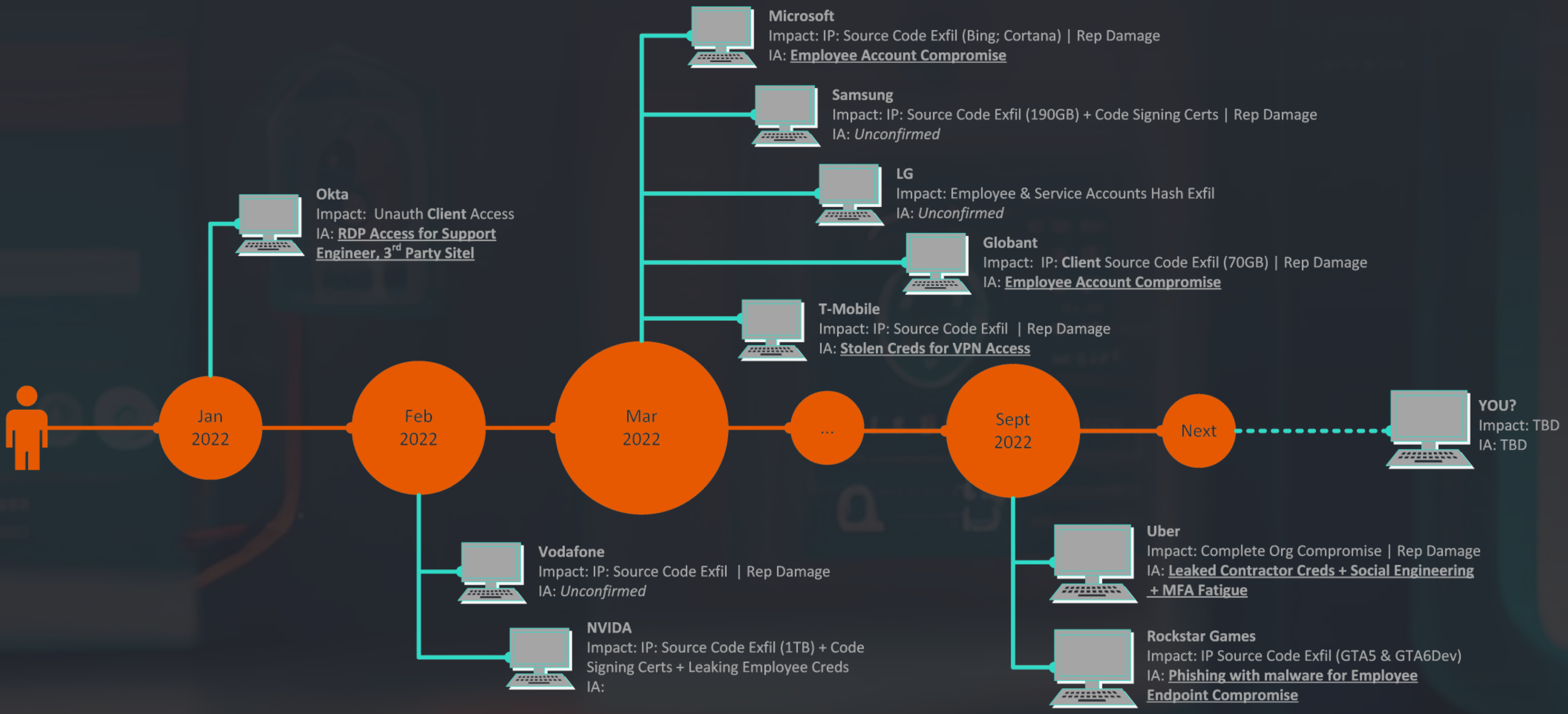
Lapsus$ is known for using many different techniques to gain initial access to an organization. The group has deployed a variety of methods to gather data about organizations and its employees, including trying to hire insiders in the telecoms industry to gain access to valid credentials and using breached credentials and social engineering to access external services of the affected companies.

Using social engineering, Lapsus$ was able to access very high-profile companies and steal proprietary information. In the case of Samsung, the group leaked all of the company's source code for its flagship phone.

Overall, Lapsus$ is not a highly sophisticated group, which highlights how poor some of these companies' security controls were.

SEPTEMBER 2022 UBER INCIDENT TIMELINE

Lapsus$



Jan 2022

Okta
Impact: Unauth Client Access
IA: RDP Access for Support Engineer, 3rd Party Sitel

Feb 2022

Vodafone
Impact: IP: Source Code Exfil | Rep Damage
IA: *Unconfirmed*

NVIDA
Impact: IP: Source Code Exfil (1TB) + Code Signing Certs + Leaking Employee Creds
IA:

Mar 2022

Microsoft
Impact: IP: Source Code Exfil (Bing; Cortana) | Rep Damage
IA: Employee Account Compromise

Samsung
Impact: IP: Source Code Exfil (190GB) + Code Signing Certs | Rep Damage
IA: *Unconfirmed*

LG
Impact: Employee & Service Accounts Hash Exfil
IA: *Unconfirmed*

Globant
Impact: IP: **Client** Source Code Exfil (70GB) | Rep Damage
IA: Employee Account Compromise

T-Mobile
Impact: IP: Source Code Exfil | Rep Damage
IA: Stolen Creds for VPN Access

…

Sept 2022

Uber
Impact: Complete Org Compromise | Rep Damage
IA: Leaked Contractor Creds + Social Engineering + MFA Fatigue

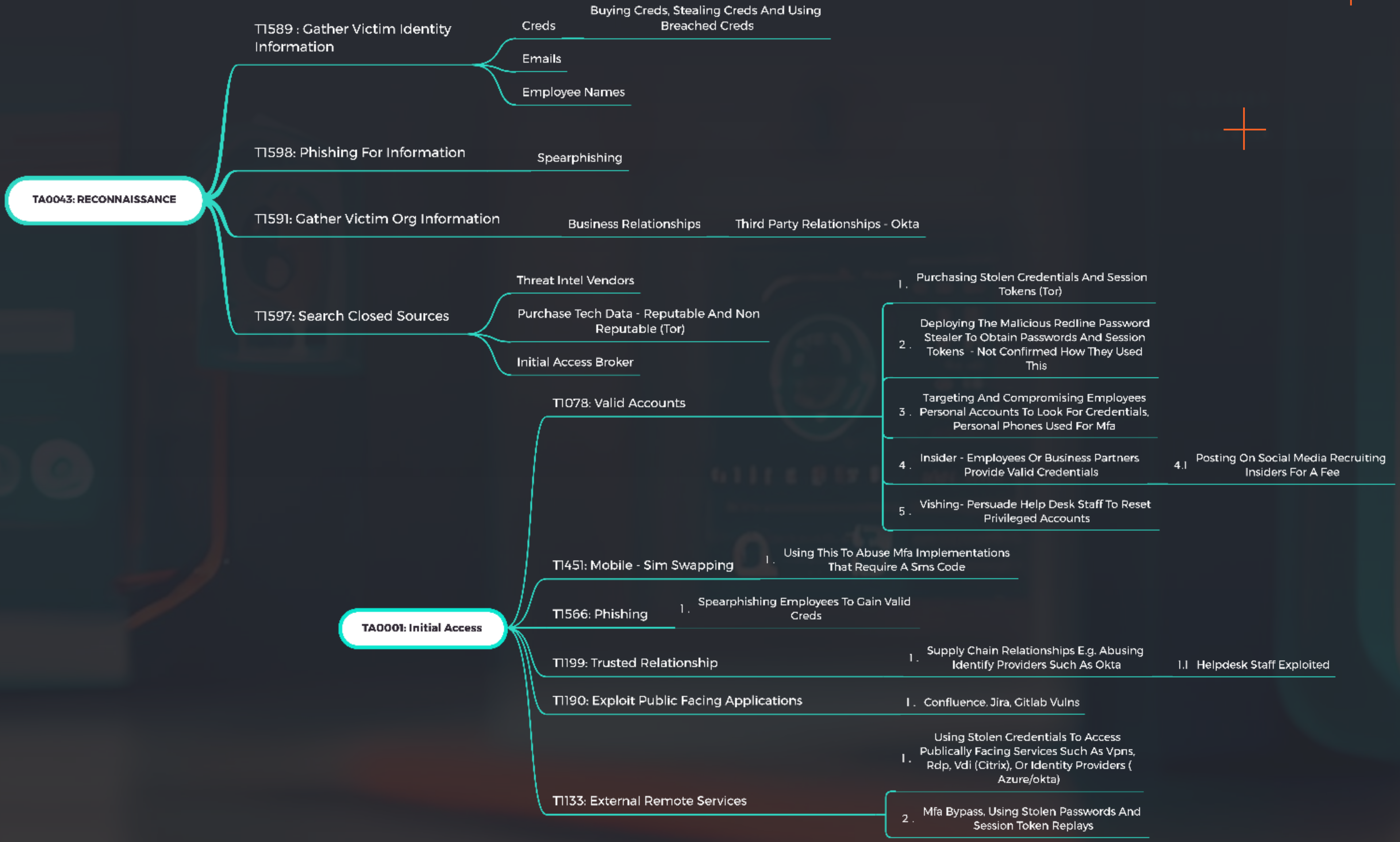
Rockstar Games
Impact: IP Source Code Exfil (GTA5 & GTA6Dev)
IA: Phishing with malware for Employee Endpoint Compromise

Next

YOU?
Impact: TBD
IA: TBD

MITRE ATT&CK TTPs

Lapsus$



- TA0043: RECONNAISSANCE
  - T1589 : Gather Victim Identity Information
    - Creds
      - Buying Creds, Stealing Creds And Using Breached Creds
    - Emails
    - Employee Names
  - T1598: Phishing For Information
    - Spearphishing
  - T1591: Gather Victim Org Information
    - Business Relationships
      - Third Party Relationships - Okta
  - T1597: Search Closed Sources
    - Threat Intel Vendors
    - Purchase Tech Data - Reputable And Non Reputable (Tor)
    - Initial Access Broker
- TA0001: Initial Access
  - T1078: Valid Accounts
    1. Purchasing Stolen Credentials And Session Tokens (Tor)
    2. Deploying The Malicious Redline Password Stealer To Obtain Passwords And Session Tokens - Not Confirmed How They Used This
    3. Targeting And Compromising Employees Personal Accounts To Look For Credentials, Personal Phones Used For Mfa
    4. Insider - Employees Or Business Partners Provide Valid Credentials
       - 4.1 Posting On Social Media Recruiting Insiders For A Fee
    5. Vishing- Persuade Help Desk Staff To Reset Privileged Accounts
  - T1451: Mobile - Sim Swapping
    1. Using This To Abuse Mfa Implementations That Require A Sms Code
  - T1566: Phishing
    1. Spearphishing Employees To Gain Valid Creds
  - T1199: Trusted Relationship
    1. Supply Chain Relationships E.g. Abusing Identify Providers Such As Okta
       - 1.1 Helpdesk Staff Exploited
  - T1190: Exploit Public Facing Applications
    1. Confluence, Jira, Gitlab Vulns
  - T1133: External Remote Services
    1. Using Stolen Credentials To Access Publically Facing Services Such As Vpns, Rdp, Vdi (Citrix), Or Identity Providers (Azure/okta)
    2. Mfa Bypass, Using Stolen Passwords And Session Token Replays

PICNIC'S INCIDENT ANALYSIS

Using Picnic's technology platform, we were able to gather and analyze data from a sample of 2,967 US-based Uber employees with different seniority levels throughout the organization. We also identified indicators of attack that point to threat actors acquiring infrastructure to launch a phishing campaign. For the attacker to be successful in this breach, they needed to find real phone numbers and employee credentials.

Key Findings

- **1,751 Uber employees** have one or more phone numbers that are readily available online that can be leveraged in a smishing attack.
- Of the **2,967 employees** sampled, 359 employees have been in data breaches.
- Picnic found **91 suspicious Uber lookalike domains**. Using our platform, we can visualize this risk and drill down into each domain to find out more information.

UBER STEALER LOGS ANALYSIS

In the September 2022 Uber breach the attacker was able to leverage stolen credentials from a contractor's device after it was infected with malware. Attackers can buy credentials or steal them using info stealer malware. This malware can be installed through various means such as when a user downloads a program that has been tampered with, or via an email in which a user is prompted to install it. Once the malware is installed, it will harvest login credentials, session tokens, and other information on the device and send this back to the attacker who will then use these credentials or sell them.

Based on our analysis, we found that 36 devices associated with Uber employees have had stealer malware installed on their devices. Uber URLs, login names, passwords, operating system details, cookies, and other files were found on these devices, including third party credentials that use an Uber email address to login in with, providing information on Uber's vendors. This information is extremely valuable to attackers as they can use these details to create a convincing pretext to socially engineer an employee into giving them access to Uber's corporate network.

It is recommended that these employees are reviewed to ensure that all their corporate credentials are changed as soon as possible to prevent attackers from leveraging this information.

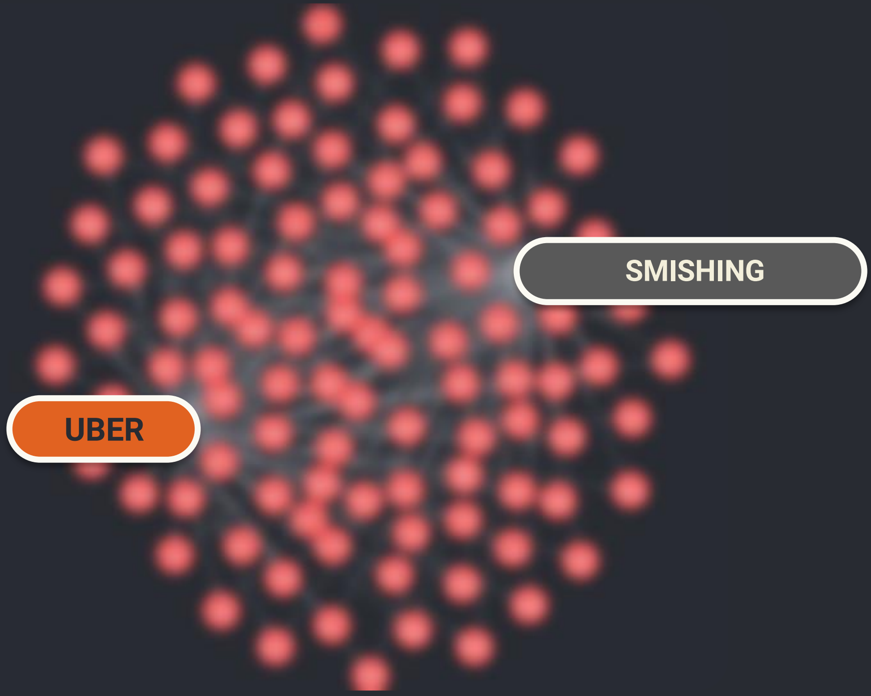
PICNIC HUNTING FOR RECON

Smishing Risk View: 1,751 employees

Of the 2,967 Uber employees whose details we have found, 1,751 of these employees have one or more phone numbers exposed on the internet.

The attacker in the Uber breach was able to leverage these exposed numbers and connect with the contractor via WhatsApp in order to launch a social engineering attack that resulted in the contractor accepting a push notification.

Uber employees (names redacted for security) that can be targeted in a smishing attack.



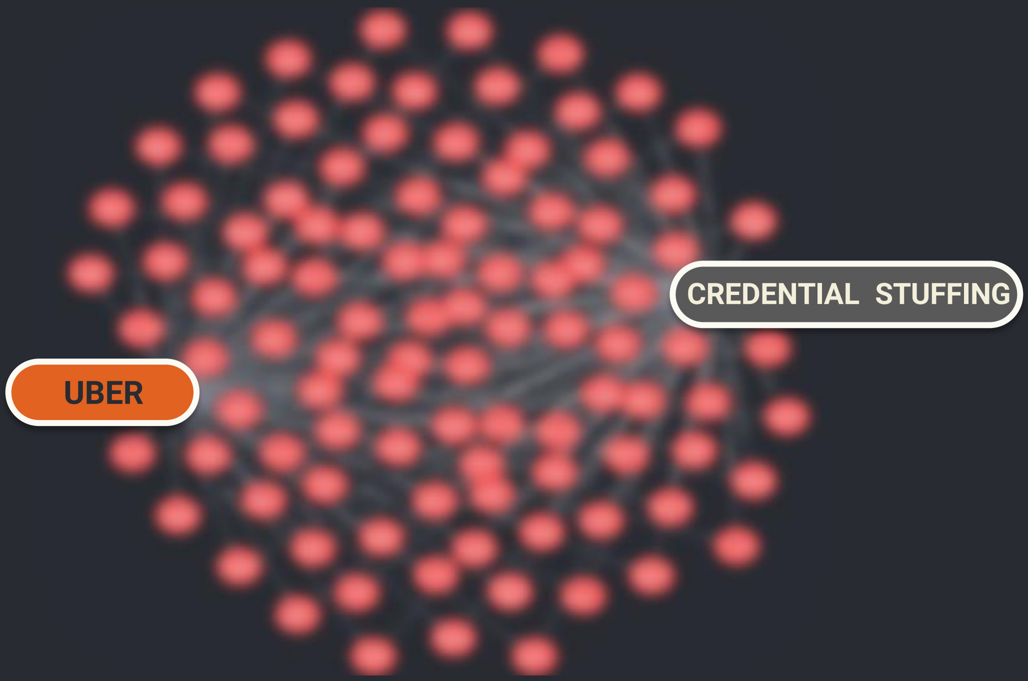
Credential Stuffing Risk View: 359 employees

Of the 2,967 Uber employee details we analyzed, 359 of these employees have breached credentials that have been exposed in one or more breaches.

238 of these employees have evidence of password reuse since the same password was found in separate breach databases.

● Threat Type ● Employee ● Company

Uber employees (names redacted for security) that can be targeted in a credential stuffing attack.



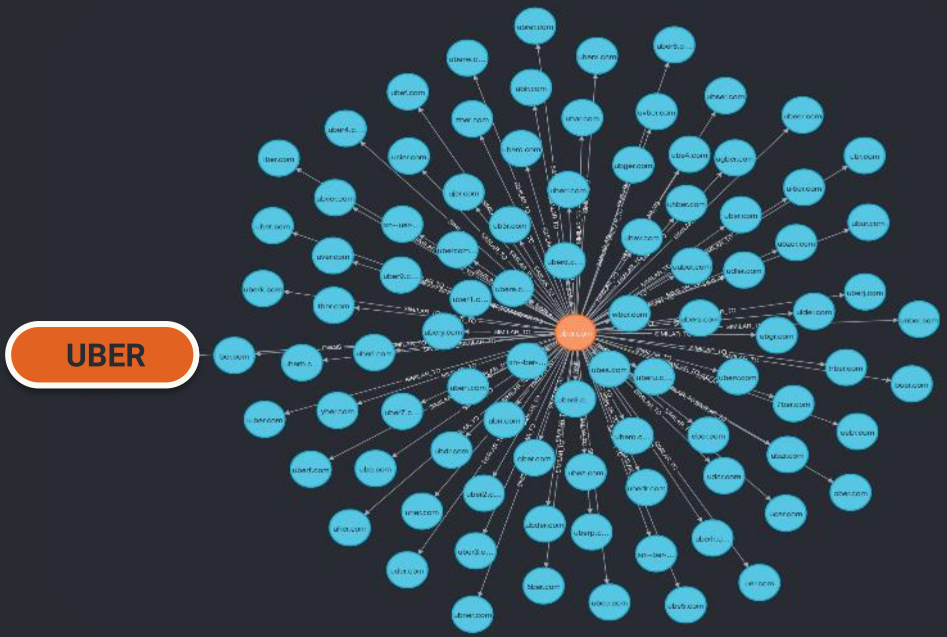
PICNIC IoATTACK

Suspicious Domains View: 91

Picnic found 91 registered suspicious Uber lookalike domains. To determine if a domain is suspicious, we look at the WHOIS record to see who registered the domain, when it was registered, and the reputation.

If an attacker is preparing to launch an attack, it is highly likely that new lookalike domains will be registered together. It is important to identify these as soon as possible so that organizations can take action to block domains before they can be used.

● Company ● Company Domain ● Suspicious Domain



1. ubes.com
2. ubez.com
3. ober.com
4. ubir.com
5. ubercom.com
6. buer.com
7. uebr.com
8. u.ber.com
9. uher.com
10. uner.com
11. ubsr.com
12. ubee.com
13. ub3r.com
14. hber.com
15. ube5.com
16. ubzr.com
17. ubrr.com
18. 7ber.com
19. uver.com
20. ubet.com
21. iber.com
22. zber.com
23. ubef.com
24. yber.com
25. ube4.com
26. uuber.com
27. ubeer.com
28. ube.com
29. ber.com
30. ubr.co
31. uer.com
32. ubrer.com
33. ubver.com
34. ubser.com
35. unber.com
36. ubner.com
37. ubger.com
38. uhber.com
39. ubzer.com
40. ugber.com
41. ubder.com
42. uvber.com
43. ubedr.com
44. xn--uer-osb.com
45. xn--ber-coa.com
46. ucler.com
47. xn--ber-3na.com
48. udcr.com
49. ulder.com
50. uder.com
51. uiber.com
52. udler.com
53. ubdr.com
54. ubar.com
55. ubgr.com
56. uber1.com
57. uberl.com
58. uberj.com
59. ubere.com
60. uberi.com
61. uber6.com
62. uberk.com
63. uberv.com
64. uberu.com
65. uberf.com
66. uber2.com
67. ubero.com
68. uber8.com
69. uberb.com
70. uberp.com
71. uber9.com
72. uberc.com
73. uberr.com
74. uber3.com
75. uber4.com
76. uberw.com
77. ubery.com
78. ubers.com
79. uber7.com
80. uberd.com
81. uberh.com
82. uberx.com
83. ujer.com
84. ubur.com
85. wber.com
86. 5ber.com
87. eber.com
88. qber.com
89. ubev.com
90. ucer.com
91. tber.com

MITIGATIONS

For Existing Picnic Customers

REDUCE EMPLOYEE ATTACK SURFACE

- Enroll employees in CheckUp to continually reduce exposed PII, neutralize exposed credentials, and ensure social media operational security.
- Enable MFA on all accounts.

MITRE Ref: T1589; T1593
MITRE Mitigation: M1056 [Pre-Compromise]

REDUCE ORGANIZATIONAL ATTACK SURFACE

- Review suspicious domains identified by Picnic and block newly registered domains similar to your organization's.
- Review Picnic’s risk assessment of any external facing components and take any recommended remedial actions.
- Review improper DNS DMARC settings identified by Picnic and ensure the correct settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.
- Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possi ble.
- Regularly audit employee access to one of least privilege (including offboarding), especially for at-risk users identified by Picnic.
- Regularly audit 3rd party access to one of least privilege, especially for at-risk users identified by Picnic.
- Monitor and neutralize sensitive information disclosure identified by Picnic, such as exposed passwords associated with personal and org breached credentials.

MITRE Ref: T1592; T1589: T1590; T1591; T1596
MITRE Mitigation: M1056 [Pre-Compromise]

MITIGATIONS

For Non-Picnic Customers (Recon)

REDUCE EMPLOYEE ATTACK SURFACE

- Ensure any breached credentials are remediated to stop password reuse.
- Review online exposure and ensure personal details are removed.
  - These can be leveraged to build trust.
  - For info that can't be removed, e.g., conference presentations, be aware of how these can be leveraged.
- Enable MFA on all personal accounts to prevent account compromise.
- Use different emails and photos for different online activity.
  - Disrupts data aggregation, including reverse image lookup.
- User awareness: If it's too good to be true, it's probably phishing.

MITRE Ref: T1589; T1593
MITRE Mitigation: M1056 [Pre-Compromise]

REDUCE ORGANIZATIONAL ATTACK SURFACE

- Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is enabled for all accounts.
- Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.
- Regularly audit employee access to one of least privilege (including offboarding).
- Regularly audit 3rd party access to one of least privilege.
- Monitor and remove sensitive information disclosure.

MITRE Ref: T1592; T1589: T1590; T1591; T1596
MITRE Mitigation: M1056 [Pre-Compromise]

For Non-Picnic Customers (IoAttack)

REDUCE EMPLOYEE ATTACK SURFACE

- Identify and block newly registered domains similar to your organization's.
  - This way if used in an attack (e.g., user clicking), the request to domain is blocked.
- Monitor for expiring domains which could be leveraged for the above.
- Expand monitoring to include trusted 3rd parties.
  - This ensures your ecosystem is pro-actively monitored and protected.
  - This can also prevent C2 comms, cred harvesting
- Use Time-Stamp Pivoting to determine domains registered together.

MITRE Ref: T1583.001
MITRE Detection: DS0038

REDUCE ORGANIZATIONAL ATTACK SURFACE

- Identify and block suspicious accounts:
  - Tied to your organization pages
  - Claiming to work for you
  - Befriending employees
  - Detections:
    - Profile creation date
    - Multiple new connections
    - Organization side, multiple connection request
    - Profile picture, eyes not legitimate / reverse image search

MITRE Ref: T1585.001
MITRE Detection: DS0021

OTHER UBER INCIDENTS

January 2023

In April 2023 it was announced in the news that Uber had suffered a new data breach in which Uber drivers' details were stolen from the IT systems of Genova Burns, a third-party law firm.

Genova Burns informed affected drivers in a letter that they were compromised when an unauthorized party gained access to the company's systems between January 23rd, 2023, and January 31st, 2023. The law firm informed Uber of this breach in March 2023 after investigating which drivers were affected and reviewing its security measures. The data that was breached included names, social security numbers, and tax numbers for drivers that the law firm held as part of their legal representation of Uber.

Uber released a statement to online news outlet The Register which said the affected drivers were ones who had completed trips in New Jersey and that they had been notified. At this time Genova Burns believes there is no evidence to suggest that this data has been misused by the attacker, but the law firm has offered 12 months of free credit monitoring for the affected drivers.

This incident highlights the importance of a trusted third party's security hygiene since vendors can pose a significant risk to affiliated organizations if they are breached.

December 2022

On December 10th, 2022, a new data breach of Uber appeared on a popular breach forum. According to Bleeping Computer, the breached data included source code, IT asset management reports, data destruction reports, windows domain login names, and emails. There were also over 77,000 details on Uber employees exposed as a result of this breach.

Uber reported this breach to be unrelated to the September breach. The December breach involved a third-party vendor and did not involve code managed by Uber. The third-party vendor that was breached was Teqtivity, who specializes in IT asset management.

https://www.theregister.com/2023/04/03/uber_drivers_info_stolen/

OTHER UBER INCIDENTS CONT.

A statement from the vendor stated that the hacker was able to get access to their AWS backup server, which hosted code and customer data. The data that was exposed consisted of customer device information and user information (names and emails). Teqtivity is currently forensically investigating the incident as well as conducting security testing on their infrastructure in response to this hack.

This incident highlights the importance of a trusted third party's security hygiene since vendors can pose a significant risk to affiliated organizations if they are breached.

The information of Uber assets and employees can be very helpful to an attacker performing recon on Uber since it allows the attacker to tailor payloads to work on Uber's infrastructure and to target employees effectively.

2016

In October of 2016, Uber suffered a data breach that affected 57 million customers and drivers. It was reported that Uber paid the hackers $100,000 to not release the data publicly and to delete it.

This breach was not disclosed publicly until November 2017, after CEO Dara Khosrowshahi launched an internal investigation to understand why this had not been reported to regulators or customers. The data involved in this breach included names and drivers' licenses for about 600,000 drivers in the US, as well as details of 57 million app users' names, emails and phone numbers.

The hackers were caught in 2017 and testified against Uber's Chief Information Security Officer, Joe Sullivan, in court in order to gain a more lenient sentence.

The hackers stated that in 2016, while looking for vulnerable GitHub repositories using stolen credentials, they found access keys for Uber's company servers hosted on AWS. Using this access, they found a storage service (s3 bucket) with over 200 user data files which they then proceeded to download (2016 breached data).

OTHER UBER INCIDENTS CONT.

The hackers then demanded a $100,000 ransom from Uber, at which time they engaged in talks with Uber's security team and went on to collect the ransom and sign a non-disclosure agreement. During the process, Uber's team used this interaction to find out their real identities.

As a result of this breach, Uber was fined $148 million. Uber fired Joe Sullivan in 2017 and he was subsequently charged with obstruction and hiding a felony from the authorities in 2020. In 2022, he was found guilty of these crimes and is awaiting sentencing. This is one of the first instances where a head of security was legally held accountable after a breach. The two hackers, Vasile Mereacre and Brandon Glover, were found guilty and are currently awaiting sentencing after their cooperation with the Joe Sullivan trial.

2016 UBER RESPONSE

- Investigating how the hackers abused GitHub, which led to finding credentials in the code repository for an Uber engineer that were used to gain initial access. Once Uber discovered this, they implemented MFA on GitHub and rotated AWS keys.
- Carrying out a review of GitHub to remove sensitive information and subsequently only using GitHub for open-source code.
- Enhancing the security of their AWS instances, such as identity and access permissions and auto-expiring credentials and making sure they were adhering to secure best practices on the platform.
- Attribution – uncovering the real identities of the hackers.
- Reviewing their bug bounty and incident response process to ensure that incidents are dealt with appropriately and legally.

CITATIONS

https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html
https://www.forbes.com/sites/daveywinder/2022/09/15/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
https://twitter.com/BillDemirkapi/status/1570602097640607744?t=wUuqf6wA_gKjxFcY7ALM5Q&s=19
https://arstechnica.com/information-technology/2022/09/uber-was-hacked-to-its-core-purportedly-by-an-18-year-old-here-are-the-basics/
https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/
https://www.bbc.co.uk/news/uk-england-oxfordshire-63048518
https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html
https://www.forbes.com/sites/daveywinder/2022/09/15/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
https://twitter.com/BillDemirkapi/status/1570602097640607744?t=wUuqf6wA_gKjxFcY7ALM5Q&s=19
https://arstechnica.com/information-technology/2022/09/uber-was-hacked-to-its-core-purportedly-by-an-18-year-old-here-are-the-basics/
https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/
https://www.bleepingcomputer.com/news/security/what-the-uber-hack-can-teach-us-about-navigating-it-security/
https://www.uber.com/en-GB/newsroom/security-update/
https://www.bleepingcomputer.com/news/security/uber-suffers-new-data-breach-after-attack-on-vendor-info-leaked-online/
https://www.bloomberg.com/news/articles/2022-12-13/uber-says-its-investigating-after-vendor-hit-with-cyberattack
https://www.teqtivity.com/breach-notification-statement/
https://www.uber.com/newsroom/2016-data-incident/

CITATIONS CONT.

https://www.bbc.co.uk/news/technology-42075306
https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data
https://www.courthousenews.com/hacker-details-plot-to-breach-ubers-data-servers-at-trial/
https://www.justice.gov/usao-ndca/pr/uber-enters-non-prosecution-agreement
https://www.justice.gov/usao-ndca/pr/florida-man-and-canadian-national-plead-guilty-hackingextortion-conspiracy
https://www.commerce.senate.gov/services/files/7d70e53e-73e9-4336-a100-67b233084f12
https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data
https://www.courthousenews.com/hacker-details-plot-to-breach-ubers-data-servers-at-trial/
https://www.justice.gov/usao-ndca/pr/uber-enters-non-prosecution-agreement
https://www.justice.gov/usao-ndca/pr/florida-man-and-canadian-national-plead-guilty-hackingextortion-conspiracy
https://www.commerce.senate.gov/services/files/7d70e53e-73e9-4336-a100-67b233084f12
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://unit42.paloaltonetworks.com/lapsus-group/
https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/
https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/
https://www.theregister.com/2023/04/03/uber_drivers_info_stolen/
https://www.siliconrepublic.com/enterprise/uuber-data-breach-driver-info-stolen-law-firm-genova-burns
https://www.techradar.com/news/uber-has-internal-data-stolen-in-yet-another-cyberattack

APPENDIX

HUMAN ATTACK SURFACE MANAGEMENT PLATFORM

Automated risk detection, prioritization, and mitigation

Social engineering remains the top technique used by threat actors that leads to cybersecurity breaches worldwide, resulting in successful ransomware attacks, sabotage, compromised data, reputational damage, and financial losses.

If 92% of cyberattacks are specifically crafted from the data tied to the human element, imagine the impact of knowing, managing, and reducing your human attack surface.

Picnic offers a frictionless cybersecurity solution that mitigates the threat of social engineering by proactively disrupting attacker reconnaissance and resource exploitation, effectively reducing the human attack surface at an enterprise-wide scale.

Why Picnic?

RISK VISIBILITY

Identify the resources most at risk and see the human attack surface through the lens of the social engineer to identify high-value targets and pathways to compromise.

RISK REDUCTION

Manage risk effectively by taking control of your organization's OSINT exposure and empowering HVTs, employees, and supply chain contractors to do the same with their exposure.

PREDICTION & PREVENTION

Eliminate target opportunities and attacker motives. Defend forward by preventing the compromise of users with Privileged Technical Access, wire fraud, credential stuffing, and identity theft, among other threats.

PERFORMANCE

Improve prediction and prevention by automating continuous risk detection for fewer active threats to detect and respond to.

EMPLOYEE PRIVACY & AWARENESS

Enable learning and aha moments through private and personalized risk assessments and recommendations via CheckUp, Picnic's employee facing portal.

SAVINGS

Reduce the operating costs of the cybersecurity program downstream by denying attackers the most attractive ingress vector to corporate and personal data and devices.

READY TO GET STARTED?
Schedule a short demo.
getpicnic.com/schedule-demo

METHODOLOGY

We Use Picnic's Methodology To Gather And Analyze Data About Organizations And Their Employees

1. HUNTING FOR RECON (ORG EXPOSURE)

(a) Employee footprint

(b) Organizational footprint

(c) 3rd Party footprint

2. HUNTING FOR IoATTACK (ATTACKER EXPOSURE)

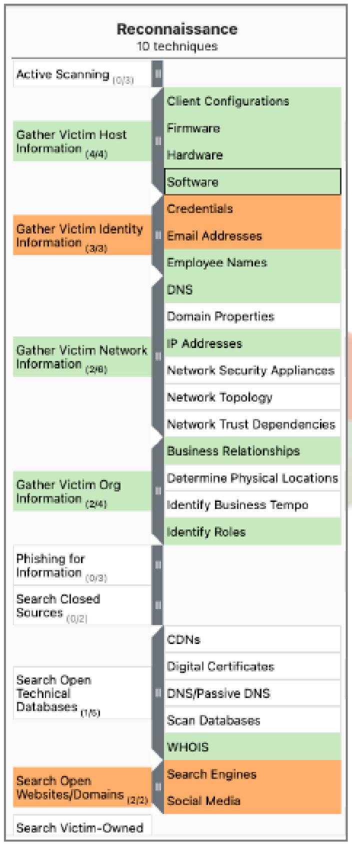
(a) Acquired Infrastructure Domains

(b) Established Accounts

PICNIC'S HUNTING FOR RECON

Org Exposure

1.



Reconnaissance
10 techniques

Active Scanning (0/3)	
Gather Victim Host Information (4/4)	Client Configurations Firmware Hardware Software
Gather Victim Identity Information (3/3)	Credentials Email Addresses Employee Names
Gather Victim Network Information (2/6)	DNS Domain Properties IP Addresses Network Security Appliances Network Topology Network Trust Dependencies
Gather Victim Org Information (2/4)	Business Relationships Determine Physical Locations Identify Business Tempo Identify Roles
Phishing for Information (0/3)	
Search Closed Sources (0/2)	
Search Open Technical Databases (1/5)	CDNs Digital Certificates DNS/Passive DNS Scan Databases WHOIS
Search Open Websites/Domains (2/2)	Search Engines Social Media
Search Victim-Owned	

EMPLOYEE EXPOSURE

- Name
- Email
- Role [access & value]
- Breached Data [password reuse]
- Interests [emotional ties]
- Associates [trust relationships]

T1589; T1593

ORG EXPOSURE

- External Remote Services [potential entry points]
- Impersonation Ability
- 3rd Party Suppliers / Trusted Relationships
- Technology Stack

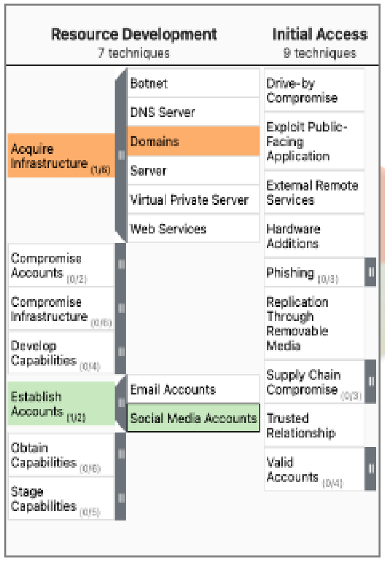
T1592; T1589: T1590; T1591; T1596

WEAPONIZATION

PICNIC'S HUNTING FOR IoATTACK

Attacker Exposure

2.



Resource Development
7 techniques

- Acquire Infrastructure (1/6)
  - Botnet
  - DNS Server
  - Domains
  - Server
  - Virtual Private Server
  - Web Services
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (1/2)
  - Email Accounts
  - Social Media Accounts
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

ACQUIRED INFRASTRUCTURE: DOMAINS

Monitor for newly registered domains similar to the org's & known 3rd parties.

- Registering a domain similar to the target is one of the first steps an attacker takes.
- This is done to disguise inbound/outbound traffic from the target.
- This also could be used for credential harvesting. By identifying the domain earlier, we can anticipate from where the attacks would generate.

T1583

ESTABLISHED ACCOUNTS: SOCIAL MEDIA

- Identify and block suspicious accounts, a.k.a. sock puppets or honey traps.
- These are used to build trust and socially engineer the target into performing an action (e.g., clicking a link).
- This is a common technique used to engage the target outside of the org's traditional security controls (e.g., social media / LinkedIn).

T1585.001 & T1566.003

INITIAL ACCESS

PICNIC'S ATTACK PREDICTION AND MITIGATION FRAMEWORK

DATA COLLECTION

Hunting for Recon

- OSINT on Employees
- OSINT on Target Org
- OSINT on Supply Chain

DATA ANALYSIS

- High Value Targets
- Data Aggregation
- Hunting for IoAttack
- Threat Intelligence

IDENTITY ATTACK SURFACE RISK

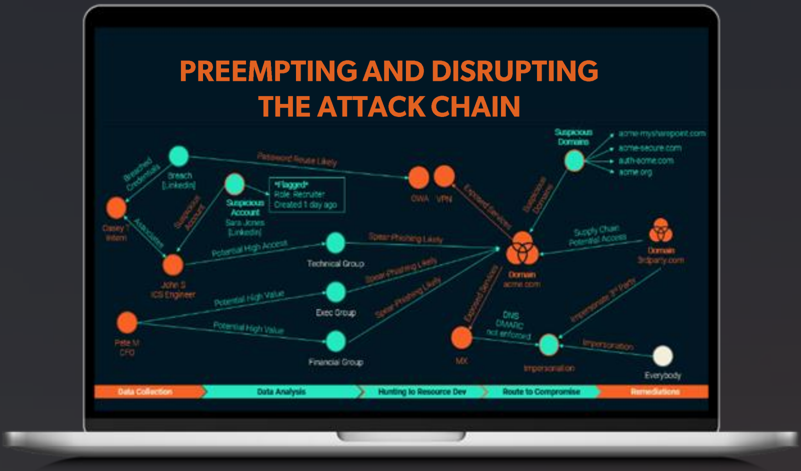
- Expose Paths to Compromise
- Prioritize Paths to Compromise

MITIGATIONS

Prioritized mitigation to reduce mean time to mitigate and reduce attack surface

- User Awareness
- User Reduced Attack Surface
- Security Team Awareness
- Org Reduced Attack Surface
- Supply Chain Awareness
- Supply Chain Reduced Attack Surface

PICNIC'S VISUALIZATION OF ATTACK AND MITIGATION FRAMEWORK



PREEMPTING AND DISRUPTING THE ATTACK CHAIN

MANIT SAHIB

Director of Global Threat Intelligence at Picnic Corporation

Manit is a Certified Red Teamer and Expert Social Engineer. Formerly Head of Red Teaming for the UK's central bank, Manit now leads Picnic's Global Threat Intelligence function, building the attacker mindset and techniques into the Picnic product line.

FELISHA MOUCHOUS

Principal Security Consultant at Picnic Corporation

Felisha is an Ethical Hacker who previously led the Penetration Testing Team for the UK's Central Bank. Felisha now works in Picnic's Global Threat Intelligence function, where she monitors and analyzes threat actor TTPs (tactics, techniques, and procedures) to enhance Picnic's product offering. She also hosts Picnic's Human Hacking 101 series.