Above our heads: How attackers are leveraging the cloud

Kim Huynh

Remi Cohen

Agenda

- Introductions
- Definitions
- Threat Landscape Details
- Case Studies
- Resources

Kim Huynh Security Program Manager

Security Research (M365 Defender for Endpoint)

- Threat Intelligence
- Incident Response
- Orchestration
- WiCyS

LinkedIn: **KimHuynhCyber**

Twitter: **@alilbyte**

Remi Cohen

@s0meGirlR3m

- Senior Threat Intelligence Engineer, F5
- Previously a red/purple teamer
- Currently researching eastern Europe, malware families, and operational technology threats

Is Cloud Security Even Real?

Yes, Of Course

But Also No

But Also Yes

Definitely Yes But Also No

Defining Cloud Security

“Unfortunately, cloud security hasn’t evolved along with the broader security and compliance infrastructure around it, and today’s world is largely unregulated or standardized. “ (InferKit, 2021)

Standardizing Definitions

"The cloud computing paradigm appears to present special security issues that will require research and careful consideration. At this point, however, these issues ***do not appear to require completely new security controls but instead the creative application of existing*** *security techniques." (Peter Mell, NIST, 2012)*

In Our Own Words

The lack of standardization, broad scope of where and how cloud applications are used, causes cloud security to **encompass all aspects** of traditional enterprise security.

We will discuss the ways in which cloud security is an important tool for attackers **at nearly every stage of and in nearly every event,** making cloud security ever-present and in defiance of a unique definition.

Cloud Security Definitions

Cloud Infrastructure

- Components needed for cloud computing.

Cloud Malware

- Programs with which cloud applications are hijacked into becoming transport mechanisms for malicious code.

Security Incident

- An event which actually or potentially jeopardizes the confidentiality, integrity, or availability of a system.

Surveys: Industry Breakdown

Top 4 Industries targeted

- Financial Services
- Technology Services
- Government
- Professional Services

Netskope: Cloud usage increased **20%**

Cloud Security Alliance: Cloud provider usage increased **13%**

Sources:

Top Threats to Cloud Computing Plus: Industry Insights | CSA (cloudsecurityalliance.org)

A SANS Survey: Network Security in the Cloud | SANS Institute

CDN Network: Benefits of Cloud Security

Key Concerns

Major Concerns:

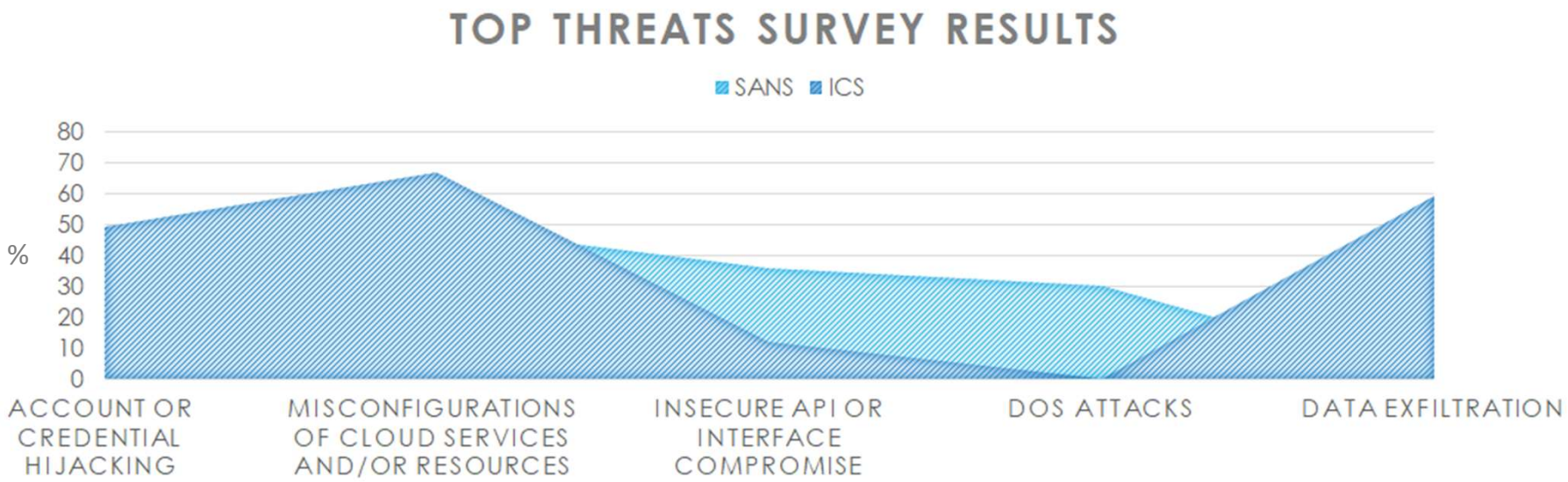
1. Unauthorized access
2. Misconfigured interfaces
3. Lack of skills or training within the organizations
4. Lack of visibility into the data processed

Reality:

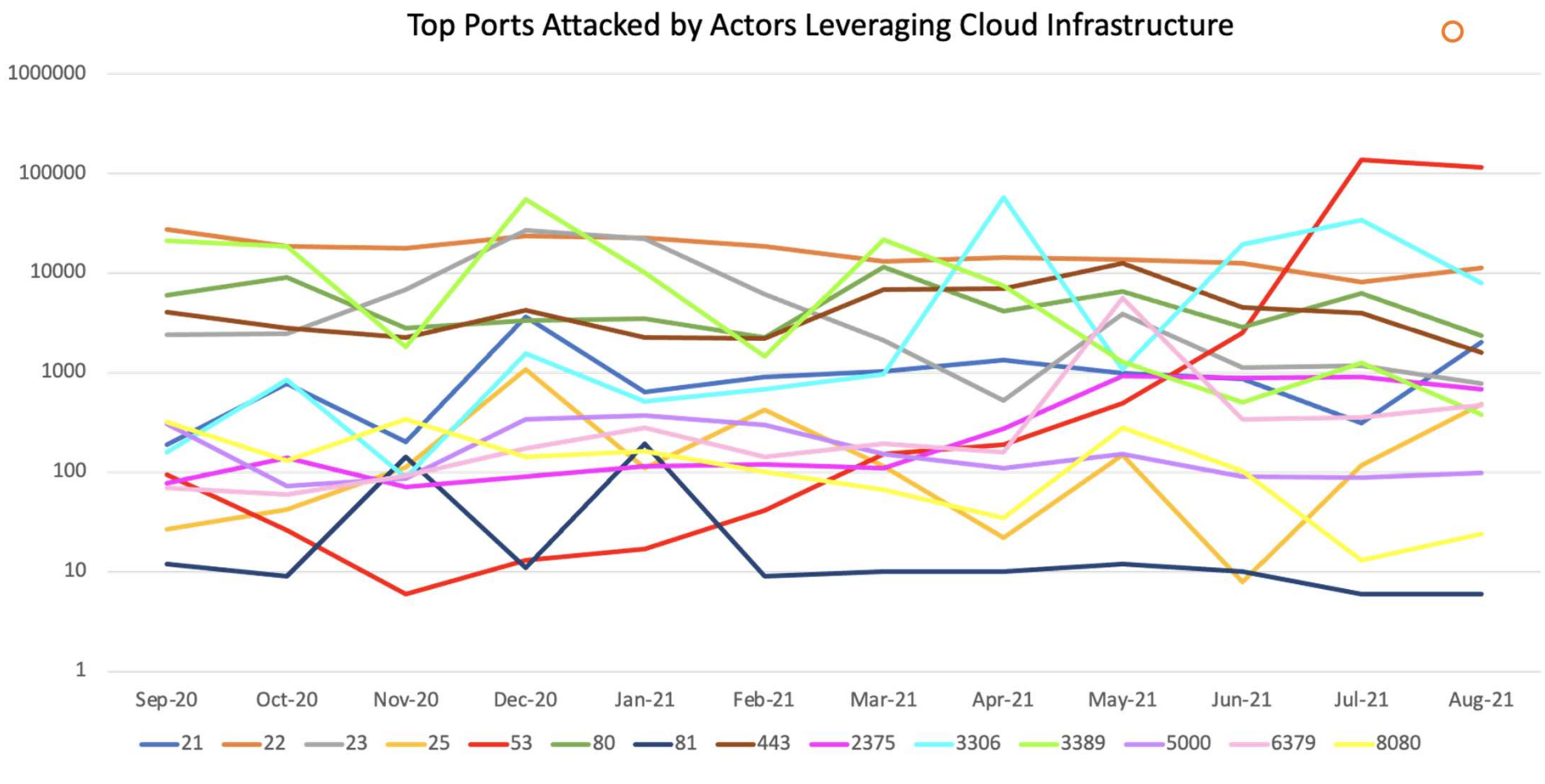
1. Lack of skills or training
2. Misconfigured interfaces and applications
3. Unauthorized access by outsiders
4. Unauthorized access by application components or compute instances

Sources: A SANS Survey: Network Security in the Cloud | SANS Institute

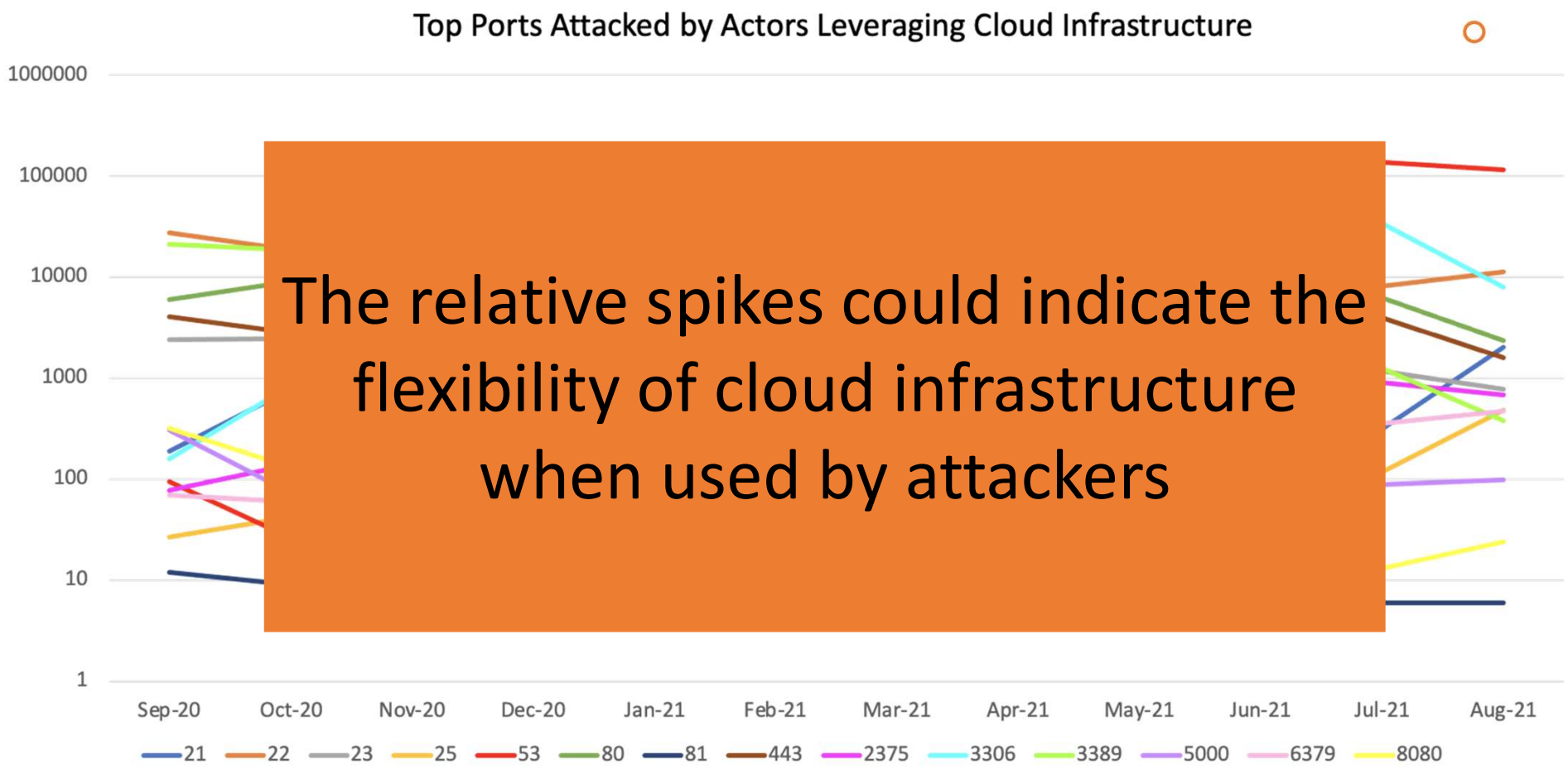
Threat Landscape Summary



Recent Attacks: Top Ports & Services

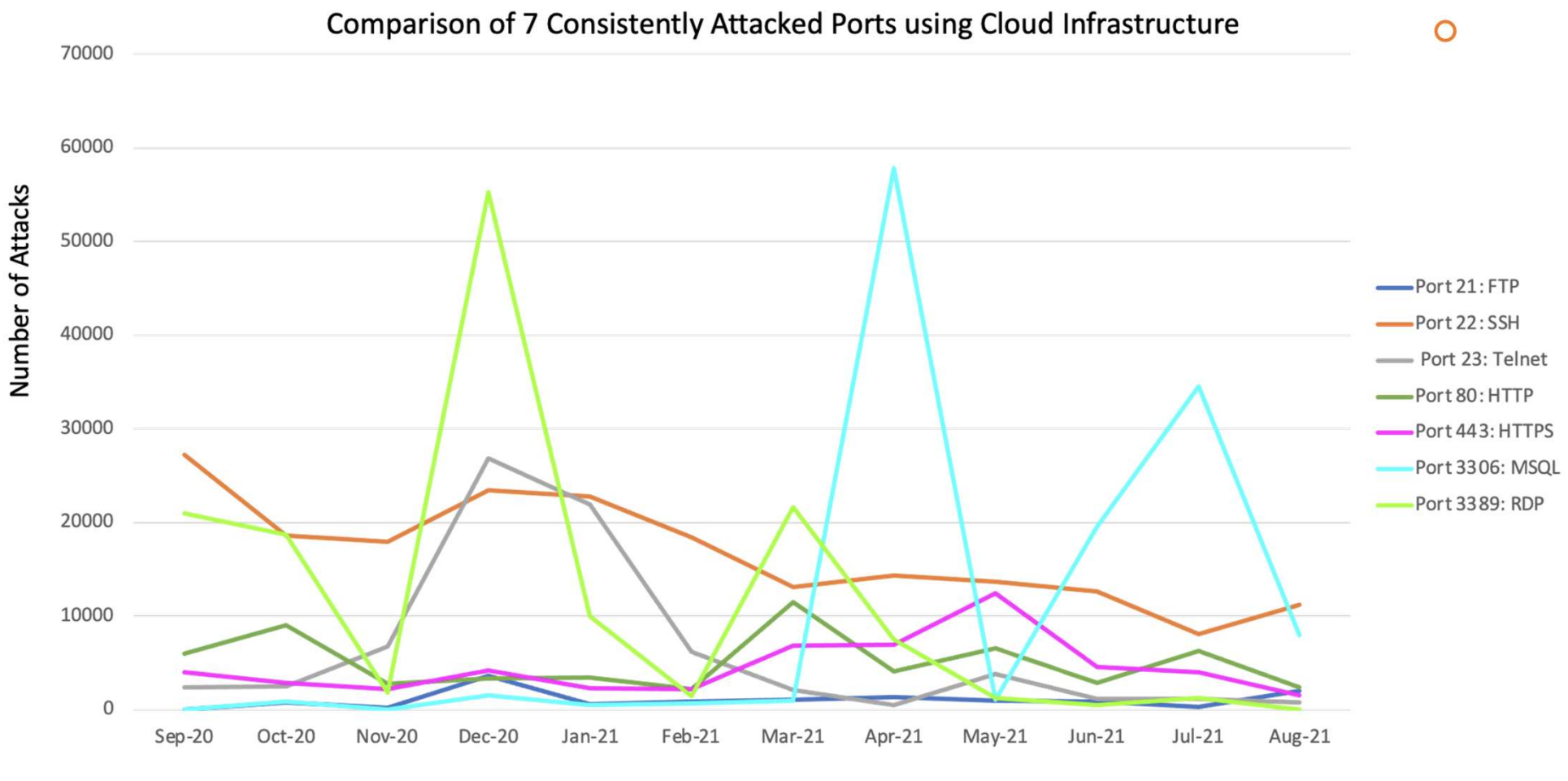


Recent Attacks: Top Ports & Services

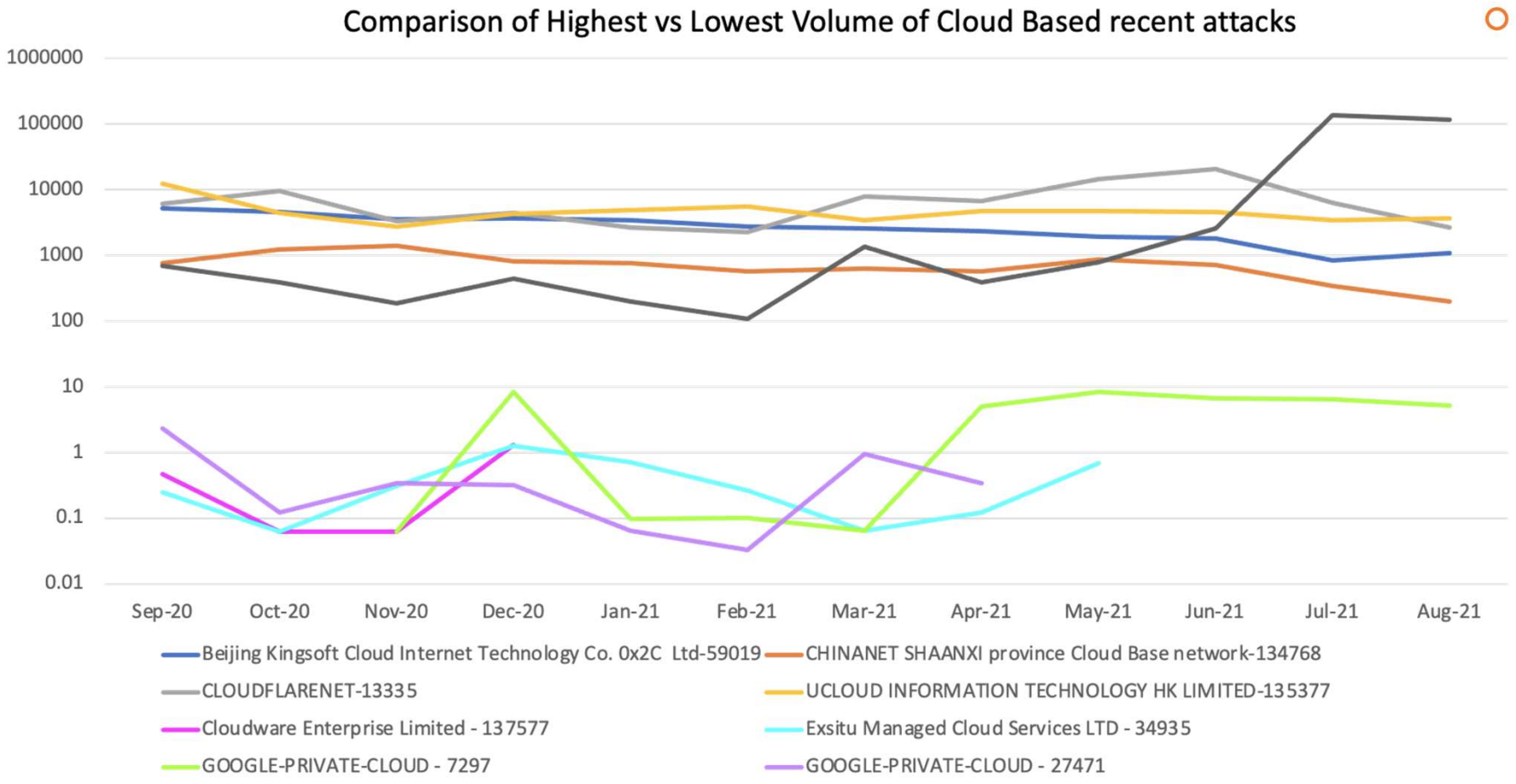


The relative spikes could indicate the flexibility of cloud infrastructure when used by attackers

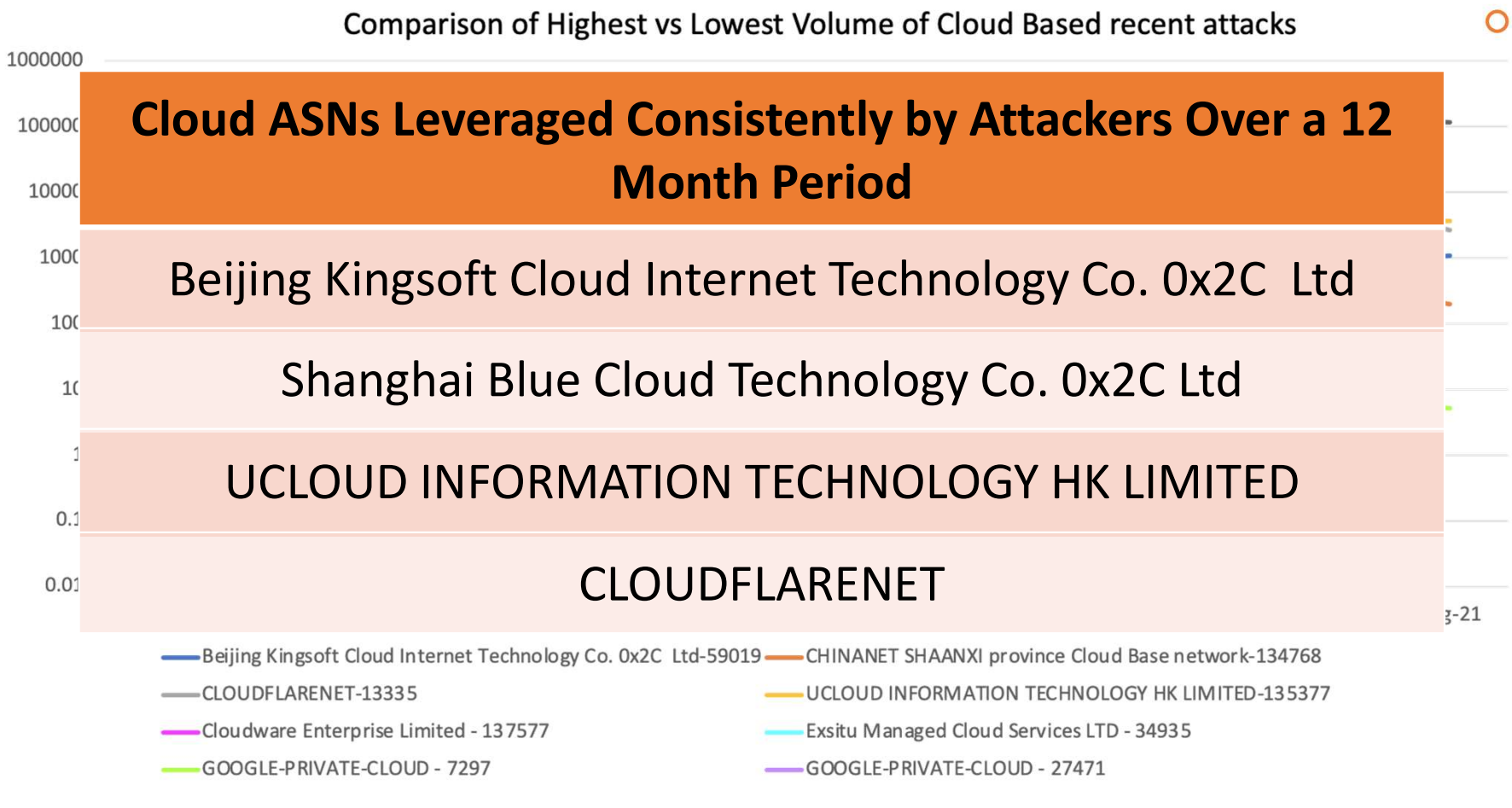
Magnitude of Recent Attacks



Recent Attacks: Cloud Infrastructure Leveraged



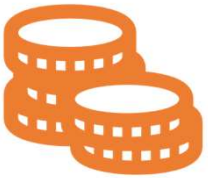
Recent Attacks: Cloud Infrastructure Leveraged



Attacker Landscape

This is just part of the story. There is more work to be done.

- Large scale attacks
- Crypto-mining
- Policy
- Availability and Cost



Impact Landscape

- Following an attack, cloud resources are valuable not only for data but for scalable resourcing for revenue generation through mining, future attacks, ad fraud, or access sale.

- Rising rates of crypto-mining botnets such as LemonDuck, Sysrv-Hello, HoleSwarm, PurpleFox, EleetHub target edge cloud services to leverage scalable resources more effectively.

Case Study

SolarWinds Orion

Impact: Widespread compromise due to a Supply Chain attack within SolarWinds Orion product

Cloud Applications: AWS and Azure in attacker infrastructure, targeting hybrid multi-cloud environments

Summary: The breadth of the SolarWinds Orion hack is unprecedented as one of the largest of its kind. Attackers leveraged cloud infrastructure to systematically carry out their attack and set up C2 servers. They also used targeted hybrid cloud environments on their victims to impersonate legitimate users. This is an example of attackers both being customers of cloud environments and abusing legitimate cloud services.

References: [media 1] [media 2] [media 3] [media 4]

Date: Discovered December 2020

Case Study
Jupyter Stealer

Impact: Widespread backdoors, credential, keystroke and information theft on enterprise systems

Cloud Applications: Amazon AWS, Google Cloud Services, CloudFlare, StrikinglyCDN

Summary: Malware propagated via widespread network of cloud-created and cloud-compromised infrastructure hosting documents via SEO. It is resilient to takedown by any major cloud providers. A single account or storage bucket can be utilized to host thousands of documents to generate advertising revenue and infect users.

References: **[Morphisec]** **[Cisco Talos]** **[Microsoft]**

Date: 2020 - Present

Case Study

Operation Cloud Hopper

Impact: MSPs breached, successful espionage attack by APT10 accessing critical data from US-based companies

Cloud Applications: Cloud Security Companies Targeted

Summary: The attackers were able to get hold of security credentials by sending phishing emails to people who worked for cloud companies. They then leveraged the access this social engineering gave them to install malware that let them steal credentials and conduct reconnaissance. Once inside cloud companies' systems, the hackers were able to find jump servers that let them access different customers' networks.

References: [media 1] [media 2] [media 3] [media 4]

Date: Discovered 2016

Call to Action: Cataloging Cloud Abuses

Cataloging of cloud incidents and instances where cloud services are abused are limited to very specific vendors, or malware that preferentially abuses or targets cloud environments is limited.

Efforts such as the OWASP Cloud Security project have been started in the past but tend to not have as widespread interest as other cataloging efforts such as Malpedia or MalwareBazaar for more general activity.

What Can Providers Do

Cloud Providers currently have **gaps in accepted reporting** for cloud threats. Providers maintain bug bounties for vulnerabilities, and generic abuse reporting, but have **limited incentives** or **structured reporting** for the security community.

We'd like to encourage any cloud service providers to collaborate in establishing security community **reporting processes, SLAs and incentives.**

Cloud Providers should establish **direct communication lines** with researchers, security organizations and other cloud providers.

Closing Thoughts

Resources to learn more:
SANS book: Practical Guide to Security in the AWS Cloud

To learn about threat hunting in the cloud:

- Threat Hunting with Microsoft O365 Logs | by Monica Nathalia | Medium
- Overview - Advanced hunting | Microsoft Docs
- Hunt for threats across devices, emails, apps, and identities with advanced hunting | Microsoft Docs
- Threat hunting with Microsoft Threat Protection

Need for cybersecurity and this is highly emphasized through Security professionals with experience in Cloud Security. Here is one way to get experience and training: Microsoft 365 Security Administrator Training (MS-500) | Learning Tree International

Special Thanks

Malcolm Heath, F5 Labs
SPAMHAUS
SANS Whitepapers

Q&A

Kim: @alilbyte
Remi: @s0meGirlR3m

Join us on Discord!

Resources

owasp-cloud-security/owasp-cloud-security: OWASP Cloud Security - Enabling conversations through threat and control stories (github.com)

CloudSecurityAlliance (github.com)

Top Threats to Cloud Computing Plus: Industry Insights | CSA (cloudsecurityalliance.org)

A SANS Survey: Network Security in the Cloud | SANS Institute

What is Special About Cloud Security? (nist.gov)

Botnet Controllers in the Cloud (spamhaus.org)

Spamhaus Botnet Threat Update: Q2-2021

Amazon Web Services - thwarting spam with a decade-old best practice (spamhaus.org)

Brute Force Attack Analysis of New Cloud Attacks | Proofpoint US

Appendix

Case Study

"Compact" Phishing Kit

Impact: Largescale credential phishing

Cloud Applications: Amazon SES, MailGun, SendGrid, Glitch.Me, Google Appspot, Google FireBase, Digital Ocean

Summary: A highly effective credential phishing kit and operation leveraging compromised and created cloud infrastructure in nearly every element of attack in order to bypass security reputation filters. By leveraging compromised cloud-mail accounts the attackers could send hundreds of thousands of phishing mails and with compromised or created cloud hosting services could assure each individual mail had multiple unique links.

References: **[WMC Global]** **[Microsoft]**

Date: 2021 - Present

Enterprise Mitigations

		Control Functions		
		Preventive	**Detective**	**Corrective**
Control Types	**Physical**	Lock physical and logical systems	Review logs of anyone accessing networking equipment	Repair physical damage quickly
	Technical	Multi- Factor Authentication Establish baseline configurations	Data loss prevention tooling	Patch programs, quarantine infected systems
	Administrative	Policies, Data access governance	Reviewing centralized logging	Implement an incident response plan, and test!