Homeland Security

National Protection and Programs Directorate
OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS
March 2017

RISKS TO CRITICAL INFRASTRUCTURE THAT USE CLOUD SERVICES

Cloud services offer a number of benefits such as scalability, high availability, and decreased ownership cost. As a result, owners and operators in several critical infrastructure sectors such as Communications, Energy, Financial Services, Information Technology, and Transportation Services have migrated in-house computing resources to cloud infrastructures. However, cloud service environments still possess many of the same potential vulnerabilities associated with internally hosted environments, as well as additional exploits to virtual systems or networks. Owners and operators of critical infrastructure need to fully understand the risk environment as they address current cloud services and consider additional migration.

Industries leading the way in cloud adoption*

Financial	Healthcare	Retail	High Tech	Telecommunications	Education	Manufacturing
55%	60%	71%	86%	78%	67%	59%

*Percentage of information technology systems—by industry—that have adopted cloud services.

Key Findings

Although cloud services and physical information technology infrastructures are vulnerable to some common attack vectors, such as Denial of Service attacks, cloud services are also potentially vulnerable to a number of unique attack vectors such as Hyperjacking. When a vulnerability is exploited, cloud service providers are often reluctant to provide incident details except what is explicitly identified in the Service Level Agreement, making incident response difficult at times.

Sample of Threats to Cloud Services

Brute Force

A malicious actor attempting a large number of possible keywords or password combinations to gain unauthorized access to a system or file.

Data Leakage

The accidental or intentional releasing of information outside its intended audience.

Denial of Service

An attack preventing legitimate users from accessing information on their computer and its network connection, or from a Websites' computers and network.

DOMØ Escalation

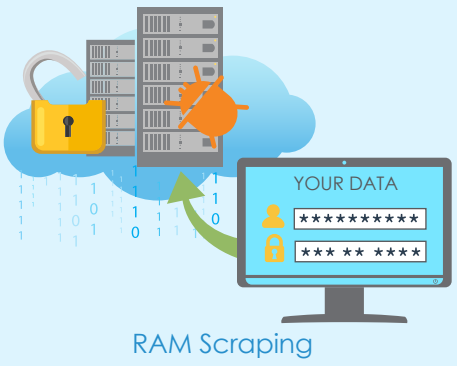
A malicious actor breaking out of the virtual environment to gain elevated access to resources that are normally protected from the user.

Hyperjacking

The successful compromise of the Hypervisor (software that manages virtual machines on a physical system) by a malicious actor, thus allowing the malicious actor to gain control of the underlying virtual machines managed by the hypervisor.

Phishing

A social engineering technique soliciting personal information from unsuspecting users. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual.



RAM Scraping

A type of malware designed for monitoring and extracting data from a system during data processing while it is unencrypted.

Virtual Machine Escape

The act of escaping a virtual machine (a virtual system or application that is running inside a physical system) and interacting directly with the virtual machine's hosting environment.

Public Cloud IaaS Hardware and Software Spending From 2015 to 2025 (in billion U.S. dollars)*

*Software as a Service (Saas); Platform as a Service (PaaS); Infrastructure as a Service (IaaS).
Source: 2016 Forbes Survey of Critical Infrastructure Sectors Using Cloud Services.

Outlook

- More rigorous security standards and development of "best practices" are necessary to assist critical infrastructure providers in understanding and managing risks to cloud-based services.
- Government and industry information technology owners and operators should consider the risks and fully vet cloud service providers before adopting or expanding current cloud-based services.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu