



CYBERARK[®]
The Identity Security Company[™]

Securing all Identities Across the Evolving Digital and Threats Landscapes

Nir Sherwinter
Director of Solutions Eng. EMEA East

April 2024

Today's world is different



Apollo Guidance Computer (AGC)

"One small step for man, one giant leap for mankind."
(Neil Armstrong, July 20, 1969)

Tech specs, then and now

The smartphone you carry in your pocket is light years ahead of the computer that guided NASA astronauts to their lunar landings. The numbers tell the tale.

APOLLO GUIDANCE COMPUTER (AGC)	DEVICE	Samsung Galaxy S10 smartphone
24" x 12.5" x 6.5"	DIMENSIONS	6" x 3" x 5/16"
70 lbs.	WEIGHT	5.5 ounces
2 kilobytes	MEMORY	8 gigabytes
Core rope memory, wires running through magnets	MEMORY TYPE	Silicon-based memory chips
Numeric display, numeric keypad (DSKY)	DISPLAY AND INPUT	High-resolution, Organic Light Emitting Diode, 3,040 by 1,440 pixels
2.048 Megahertz	PROCESSING POWER	2.84 Gigahertz

Sources: NASA, Samsung

Staff graphic

NEWS
Cha
Info
5 MINU
Yum Bra
MARC
Google Fi Wa
There's Noth
Google's cell network d
this month.

SECURITY NEWS
CYWARE SOCIAL
Alerts Events
Go to listing page
**Drone Goggles Maker O
with 'Time-bomb' Ranso
Attack**
Breaches and Incidents
• May 06, 2023
• Cyware Alerts - Hacker News

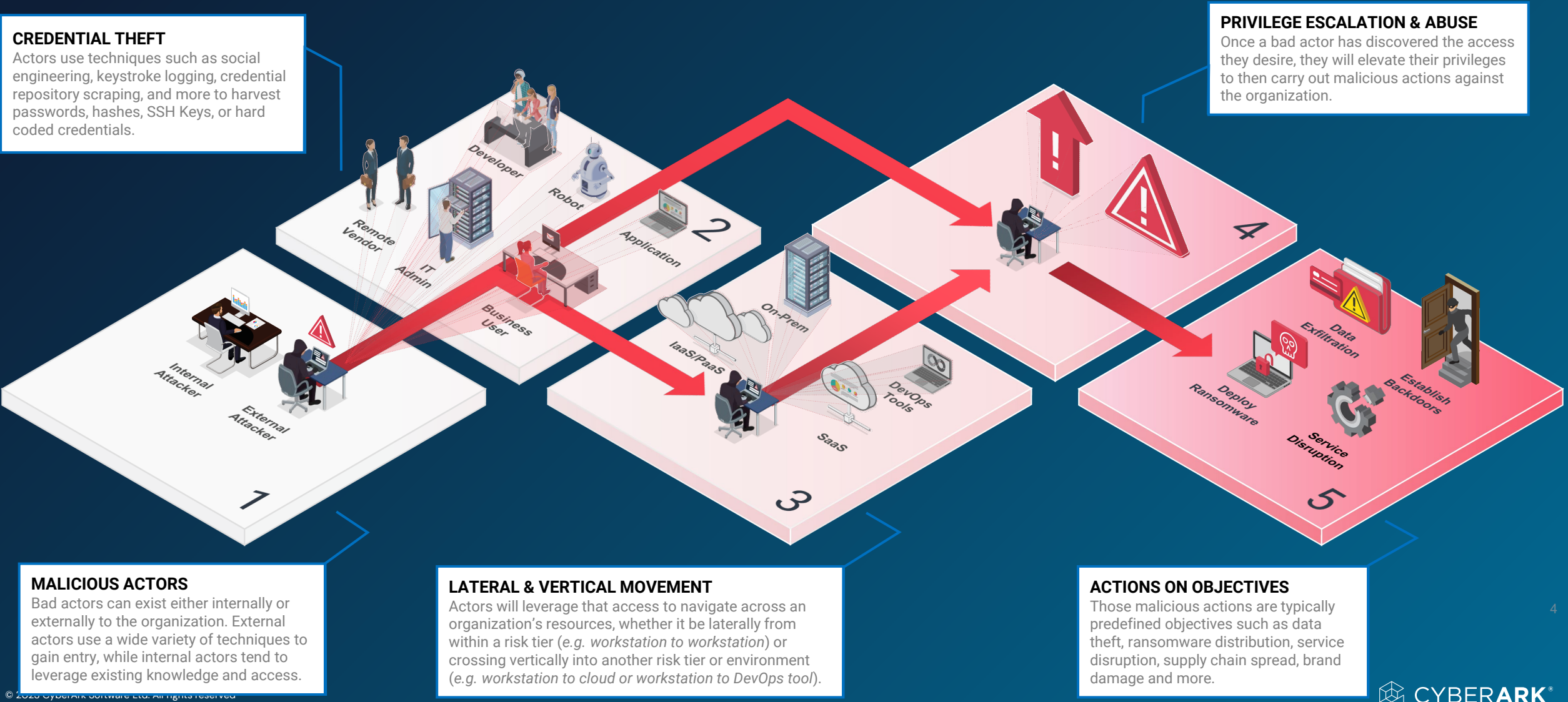
BLEEPINGCOMPUTER
Home > News > Security
> ALPHV gang claims ransomware attack on Constellation Software
Menu THE CON
**ALPHV gang cl
attack on Const**
By **Sergiu Gatlan**
May 5, 2023 11:04

The Guardian
Support us →
News Opinion Sport Culture Lifestyle
World UK Coronavirus Climate crisis Environment Science
Twitter
Twitter admits to 'security
incident' involving Circles tweets
Feature allows users to set a list of friends and post
tweets that only they are supposed to be able to read
Alex Hern UK technology editor
@alexhern
Sat 6 May 2023 10:53 BST

ars TECHNICA
SUBSCRIBE SIGN IN
HACKED AGAIN —
T-Mobile
one leak
Hack affecting
DAN GOODIN - 5/2/2023
Photo: J.K2507 (Shutterstock)
TECH
T-Mobile Add Topic +
**In latest T-Mobile hack, 37 million
customers have personal data
stolen, company says**
Wyatte Grantham-Philips
USA TODAY
Published 10:33 a.m. ET Jan. 20, 2023 | Updated 10:33 a.m. ET Jan. 20, 2023

464 shares
of their mobile app that
of users.
ck on Taiwanese
pany's private

Your Environment Evolves, Attack Chains Don't



Example – The British Library breach

The British Library is UK's national library, holds over 170 million items, including a diverse collection of Books, drawings, maps, newspapers, scripts, sound, and video recordings, etc. from private libraries dating back to the 17th and 18th centuries. It is regarded as the most important library in the world.

Attack Vector: access through VMware ESXi vulnerability of third-party suppliers.

The Rhysida ransomware gang claimed responsibility, auctioning stolen data including personal information from the CRM database; no financial data breached.

CREDENTIAL THEFT
of a 3rd party supplier

Recovery and Costs: Estimated recovery costs up to £7 million; gradual restoration of services expected to take months.
Recommendations for Affected Users: Vigilance against suspicious emails; password changes advised if used on other services.

Your Environment Evolves, Attack Chains Don't

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔗 Search Q

Thank you to SOC Prime for becoming ATT&CK's first Benefactor. To join them, or learn more about this program visit our [Benefactors page](#).

ATT&CK®

Get Started Take a Tour
 Contribute Blog 🔗
 FAQ Random Page ▾

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

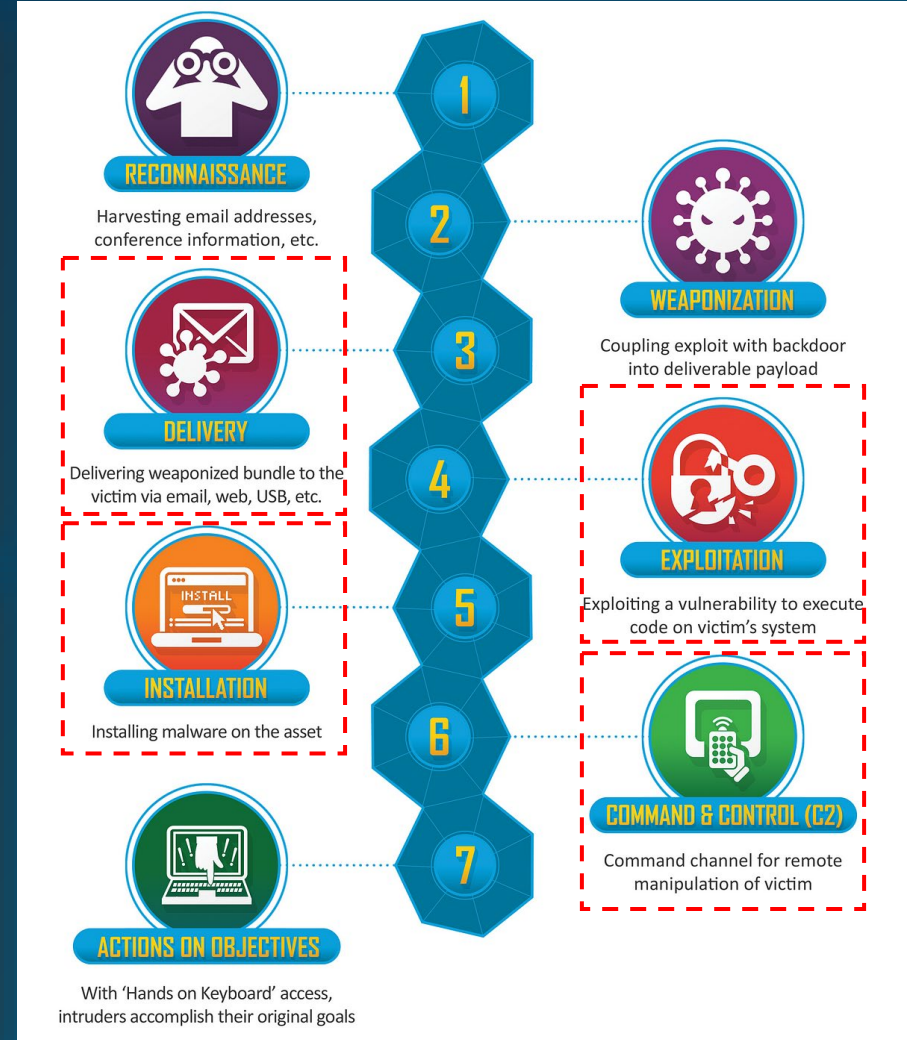
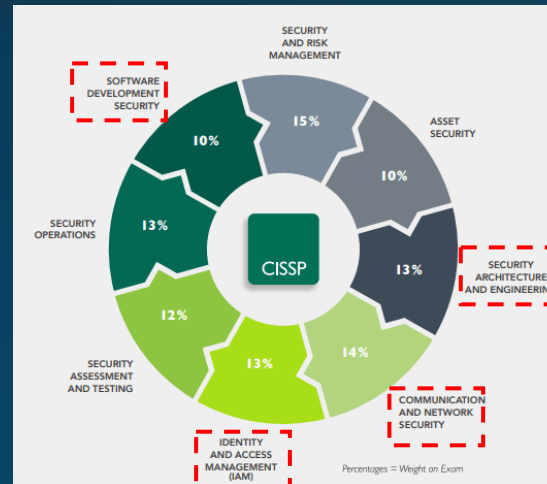
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
---------------------------------	--------------------------------------	---------------------------------	----------------------------	------------------------------	---------------------------------------	----------------------------------	------------------------------------	----------------------------	----------------------------------	-----------------------------	--------------------------------------	------------------------------	-------------------------

Adversaries use **identities** and escalate **privileges** as part of each and every attack.



90% of organizations experienced at least one identity-related incident in the past year.

Adversaries continue to attack identities and escalate **privilege** until *they* become the source of identity.

Today's **siloes approach** was built to solve yesterday's problems.



**New
Identities**



**New
Environments**



**New Attack
Methods**



Today's world
requires a
new approach.

✓ Security-first

✓ Unified

✓ All Identities

Spectrum of Secured Identities



Target Resources

Workforce

Endpoints,
Data, Biz Apps

IT

Data, Apps,
Workloads, CI/CD Tools

Developers

Data, Apps, Workloads,
Code Repos, Cloud Services

Machines

Devices, Data, Apps,
Workloads, Code

Access to data

Access and ability to change data and infrastructure

Access and ability to change data infrastructure and code

Risk of Access Level



Complexity of Access



Lower

Higher

Solutions for Securing **Every Identity**



Workforce



IT



Developers



Machines

IDENTITY SECURITY

Securing Workforce Users

Securing High Risk Users

Securing IT Admins

Securing Cloud Operations Teams

Securing Developers

Securing Cloud Workload Identities

Securing Secrets for Hybrid IT/OT

Securing Desktops & Servers

Identity Security Platform

Identities



Admins



Workforce



Third Parties



Customers



DevOps



Workloads



Devices

Resources



Applications & Services



Infrastructure & Endpoints



Data

Environments



Data Centers



OT



Hybrid & Multi-Cloud



SaaS

Seamless & Secure Access for All Identities

Intelligent Privilege Controls

Flexible Identity Automation & Orchestration



Workforce & Customer Access



Endpoint Privilege Security



Privileged Access Management



Secrets Management



Cloud Privilege Security



Identity Management

Identity Security Intelligence



Shared Services

Single Admin Portal

Workflows

Unified Audit

Authentication & Authorization

SaaS

Hybrid

Self-Hosted

Cookieless Browsing

Password Replacement

Quick Access Bar

Extensibility

**SaaS Apps, PAM Targets,
On Prem, Web Based**



Innovation & Expertise

3,000+ Employees

1,000+ in Product & Technology

8,000+ Customers

Thousands of C3 Partner Integrations

Our Mission

Deliver the world's most advanced platform to secure all identities anywhere, with intelligent privilege controls.

Thank You!