G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

DECEMBER 2020

Highlights

Coded 340 Message Sent by Zodiac Killer Cracked After 51 Years

Nuclear Labs, Pentagon, US Treasury Hacked

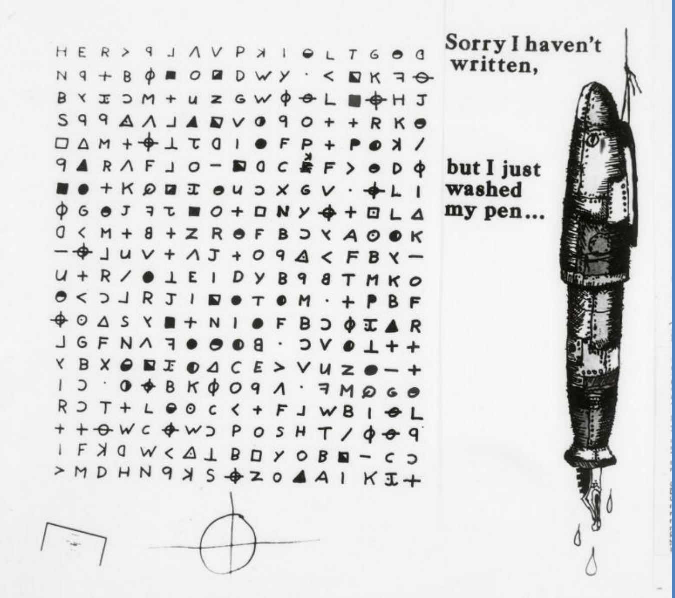
NSA Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources

AI Copilot for U-S Spy Plane

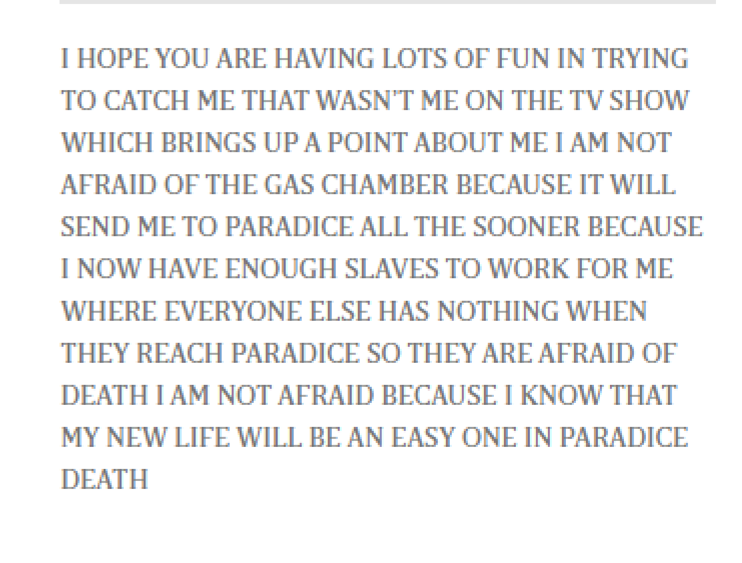
G2M Research Multi-Vendor Webinar Series – 2021 Schedule

Coded 340 Message Sent by Zodiac Killer Cracked After 51 Years

The Zodiac Killer killed at least 5 people in Northern California in 1968 and 1969. He sent letters with cryptic message to the press, claiming responsibility for 37 murders. He continued to send messages until 1974.The murders were never solved and a coded message called Z-340 or just 340, referencing the number of characters in the message, remained a mystery. Since November 1969, professional and amateur cryptographers have been trying to crack the cipher.



Sorry I haven't written, but I just washed my pen...



I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME THAT WASN'T ME ON THE TV SHOW WHICH BRINGS UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAUSE IT WILL SEND ME TO PARADICE ALL THE SOONER BECAUSE I NOW HAVE ENOUGH SLAVES TO WORK FOR ME WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADICE SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID BECAUSE I KNOW THAT MY NEW LIFE WILL BE AN EASY ONE IN PARADICE DEATH

Dave Orachak, a software developer from Virginia, Sam Blake, an applied mathematician living in Australia, and Jarl Van Eycke, a warehouse operator in Belgium, successfully cracked the transposition cipher. This technique changes the order of the letters in a text by placing it in a grid. For months, Mr. Blake said, he and Mr. Oranchak tested, by trial and error, around 650,000 possible solutions, running them through a code-breaking program written by Mr. Van Eycke. The identity of the Zodiac Killer remains a mystery.

Nuclear Labs, Petagon, US Treasury Hacked

In an ever-evolving story, it now appears that the threat actors who penetrated FireEye in early December with a highly sophisticated attack were in fact utilizing a threat payload that was deployed by a trojanized version of the SolarWinds Orion system management product. The SolarWinds tools, which are used by a number of government agencies, telcos, and other enterprises (including FireEye) were exploited through an Orion backdoor called “Sunburst”. This backdoor enabled (among other things) the theft of FireEye’s Red Team tools, a sophisticated set of penetration tools. The US Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive instructing federal agencies to immediately disconnect affected devices. The backdoor affected SolarWinds Orion version 2019.4 through 2020.2.1 HF1.

Nearly 33,000 organizations utilize the SolarWinds Orion product, including the U.S. Treasury, the U.S. Department of Commerce, though SolarWinds has said in an SEC 8-K filing on December 14th that they believe that fewer than 18,000 customers were using the versions affected by the Sunburst backdoor. SolarWinds plans to release an updated version of Orion immediately that will eliminate the malware and payloads from affected systems.

That attack has been attributed by some in the cybersecurity industry to Cozy Bear or APT29, a known unit of the Russian Federation's SVR foreign intelligence service. While the Russian government denies involvement in the attack, several cybersecurity organizations believe that the attack is too sophisticated to have come from a non-state actor. The attack utilized tools to bypass dual-factor authentication (DFA) protocols to break into Outlook email services to access emails that would help them further penetrate their targets. The attackers also utilized techniques to identify security software on the attacked systems and obfuscate the trojanized software and its payloads from detection. The result was an attack that was exceptionally difficult to detect, and which sat idle for several months before launching itself.

Microsoft said Thursday that it had identified 40 companies, government agencies and think tanks that the suspected Russian hackers, at a minimum, had infiltrated. Nearly half are private technology firms, Microsoft said, many of them cybersecurity firms, like FireEye, that are charged with securing vast sections of the public and private sector.

"I'm struggling with what the SolarWinds incident means for defending forward. How is this not a massive intelligence failure, particularly since we were supposedly all over Russian threat actors ahead of the election?"

"The IC kept reporting that the Russians were targeting the election. That didn't happen but was the evidence that they were planted? Did NSA fall into a giant honeypot while the SVR quietly pillaged the USG and industry?

Robert Knake, Whitney Shepardson Senior Fellow, Council on Foreign Relations, Director for Cybersecurity Policy at the National Security Council from 2011-2015

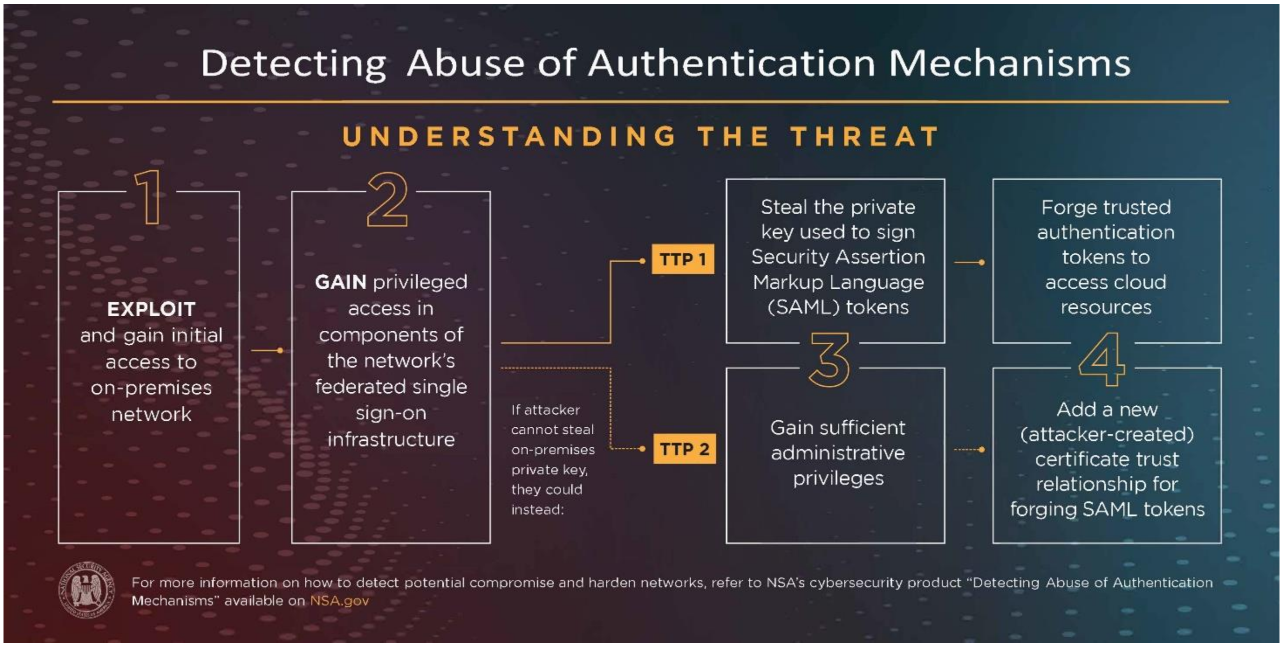
Federal officials deem this attack “a grave risk to the federal government.”

The weak point for the government computer networks remains administrative systems that have a number of private companies working under contract. By gaining access to these peripheral systems, hackers access central parts of the government networks.

SolarWinds was an easy target for hackers given they lack a chief information security officer and a researcher informed the company last year that he had uncovered the password to SolarWinds’ update mechanism, the vehicle through which 18,000 of its customers were compromised. The password was “solarwinds123.”

NSA Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources

The National Security Agency (NSA) released a Cybersecurity Advisory “Detecting Abuse of Authentication Mechanisms” Two TTPs forge authentications and gain access to a victim’s cloud resources. They require the actors to already have privileged access in an on-premises environment. Then, they can be combined with other vulnerabilities to gain initial access, to undermine trust, security, and authentication. Mitigation actions include hardening and monitoring systems that run local identity and federation services, locking down tenant single sign-on (SSO) configuration in the cloud, and monitoring for indicators of compromise.



Detecting Abuse of Authentication Mechanisms

UNDERSTANDING THE THREAT

1 **EXPLOIT** and gain initial access to on-premises network

2 **GAIN** privileged access in components of the network’s federated single sign-on infrastructure

TTP 1

Steal the private key used to sign Security Assertion Markup Language (SAML) tokens

Forge trusted authentication tokens to access cloud resources

If attacker cannot steal on-premises private key, they could instead:

TTP 2

3 Gain sufficient administrative privileges

4 Add a new (attacker-created) certificate trust relationship for forging SAML tokens

For more information on how to detect potential compromise and harden networks, refer to NSA’s cybersecurity product “Detecting Abuse of Authentication Mechanisms” available on NSA.gov

AI Copilot for U-2 Spy Plane

After over a million training runs, US Air Force flew an AI copilot on a U-2 Dragon Lady high-altitude reconnaissance spy plane in Calfornia, using an AI algorithm called ARTUu. The artificial intelligence algorithm handled sensor control, looking for enemy missile launchers. This allowed the human polot to concentrate on flying and looking for enemy aircraft. This historic flight launched just two months after the U-2 Federal Laboratory team updated inflight software for the first time during a training mission, leveraging the open-source container orchestration software, Kubernetes, another first for the military.

“Putting AI safely in command of a U.S. military system for the first time ushers in a new age of human-machine teaming and algorithmic competition,” explains Dr. Will Roper, Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics. “Failing to realize AI’s full potential will mean ceding decision advantage to our adversaries.”

The Air Force Project Maven, using AI to scan drone footage, is being incorporated into the Advanced Battle Management System (ABMS) to align AI-efforts and support broader combat capabilities. Just over two years ago, 3000 Google employees wrote an open letter urging Google to not work with the military on projects to use AI in warfare, stating that Google should not be in the business of war and the project would damage its brand and public trust. Google backed off but the DOD argued the project’s lack of transparency was the issue, more than the project itself.

Lt. Gen. Jack Shanahan, “AI is a critical component of our nation’s prosperity, vitality and self-sufficiency. In other words, no matter where you stand with respect to the government’s future use of AI-enabling technologies, I submit that we can never attain [the nation’s vision for it] without industry and academia with us together in an equal partnership. There’s too much at stake to do otherwise.”

G2M Research Multi-Vendor Webinar Series

Our 2021 webinar schedule is ready! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact G2M for a prospectus.

Our November webinar “Implementing NVME™ & NVMe-oF™ for Cloud Service Providers” was sponsored by Kioxia (Joel Dedrick), Lightbits (Josh Goldenhar), and Western Digital (Mark Miquelon). View the recording and/or download a PDF of the slides.

G2M RESEARCH

Jan 19:	Can Your Server Handle The Size of Your SSDs?
Feb 23:	Storage Architectures to Maximize the Performance of HPC Clusters
March 23:	One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?
April 20:	The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle)
May 18:	Responsive and Efficient Storage Architectures for Social Media
June 15:	It’s 2021 - Where Has NVMe-oF™ Progressed To?
July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: “And The Winner Is”?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion