Dissecting the SolarWinds Hack Without the Use of Signatures

Max Heinemeyer, Director of Threat Hunting, Darktrace

The SUNBURST malware attacks against SolarWinds have heightened companies' concerns about the risk to their digital environments. Malware installed during software updates in March 2020 has allowed advanced attackers to gain unauthorized access to files that may include customer data and intellectual property.

Darktrace does not use SolarWinds and its operations remain unaffected by this breach. However, SolarWinds is an IT discovery tool that is used by a significant number of Darktrace customers. In what follows, we explore a set of Darktrace detections that highlight and alert security teams to the types of behaviors related to this breach.

This is not an example of a SolarWinds compromise but examples of anomalous behaviors we can expect to see from this type of breach. These examples stress the value of self-learning Cyber AI capable of understanding the evolving normal 'patterns of life' within an enterprise – as opposed to a signature-based approach that looks at historical data to predict today's threat.

As Darktrace detects device activity patterns rather than known malicious signatures, detecting use of these techniques will fall into the scope of Darktrace's capabilities without further need for configuration. The technology automatically clusters devices into 'peer groups', allowing it to detect cases of an individual device behaving unusually. Using a self-learning approach is the best possible mechanism to catch an attacker who gains access into your systems using a degree of stealth so as to not trigger signature-based detection.

A number of these models may fire in combination with other models in order to make a strong detection over a time-series – and this is exactly where Darktrace's autonomous incident triage capability, Cyber AI Analyst, plays a crucial role in investigating the alerts on behalf of security teams. Cyber AI Analyst saves critical time for security teams and its results should be treated with a high priority during this period of vigilance.

Darktrace Detections

We want to focus on the most sophisticated details of the hands-on intrusion that in many cases followed the initial automated attack. This post-exploitation part of the attack is much more varied and stealthy. These stages are also near-impossible to predict, as they are driven by the attacker's intentions and goals for each individual victim at this stage – making the use of signatures, threat intelligence, or static use cases virtually useless.

While the automated, initial malware execution is a critical initial step to understand, the behaviour was pre-configured for the malware and included the download of further payloads and the connection to domain-generation-algorithm (DGA) based subdomains of avsvmcloud[.]com. These automated first stages of the attack have been sufficiently researched in depth by the community. This post is not aiming to add anything to these findings but instead takes a look at the potential post-infection activities.

Malware / C2 Domains

The threat-actor set the hostnames on their later-stage command and control (C2) infrastructure to match a legitimate hostname found within the victim's environment. This allowed the adversary to blend into the environment, avoid suspicion, and evade detection. They further used C2 servers in geopolitical proximity to their victims, further circumventing static geo-based trusts lists. Darktrace is unaffected by this type of tradecraft as it does not have implicit, pre-defined trust of any geo-locations.

This would be very likely to trigger the following Darktrace Cyber AI models. The models were not specifically designed to detect SolarWinds modifications but have been in place for years – they are designed to detect the subtle but significant attacker activities occurring within an organization's network.

- Compromise / Agent Beacon to New Endpoint
- Compromise / SSL Beaconing to New Endpoint
- Compromise / HTTP Beaconing to New Endpoint*

*The implant uses SSL but may be identified as HTTP if using a proxy.

Lateral Movement Using Different Credentials

Once the attacker gained access to the network with compromised credentials, they moved laterally using multiple different credentials. The credentials used for lateral movement were always different from those used for remote access.

This very likely would trigger the following Cyber AI models:

- User / Multiple Uncommon New Credentials on Device

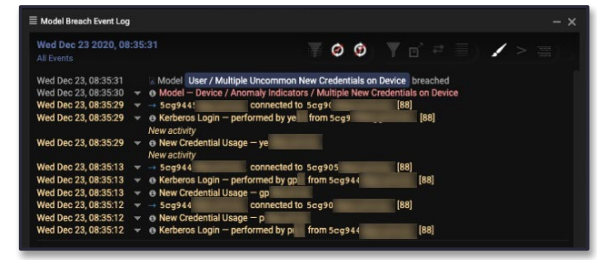

Figure 1: Example breach event log showing anomalous (new) logins from a single device, with multiple user credentials

- User / New Admin Credentials on Client

Figure 2: Example breach event log showing anomalous admin login

Temporary File Replacement and Temporary Task Modification

The attacker used a temporary file replacement technique to remotely execute utilities: they replaced a legitimate utility with theirs, executed their payload, and then restored the legitimate original file. They similarly manipulated scheduled tasks by updating an existing legitimate task to execute their tools and then returned the scheduled task to its original configuration. They routinely removed their tools – including the removal of backdoors once legitimate remote access was achieved.

This would be very likely to trigger the following Cyber AI models:

- Anomalous Connection / New or Uncommon Service Control

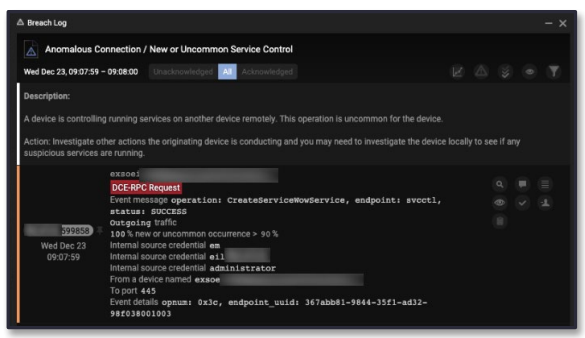

Figure 4: Example breach showing uncommon service control

- Anomalous Connection / High Volume of New or Uncommon Service Control

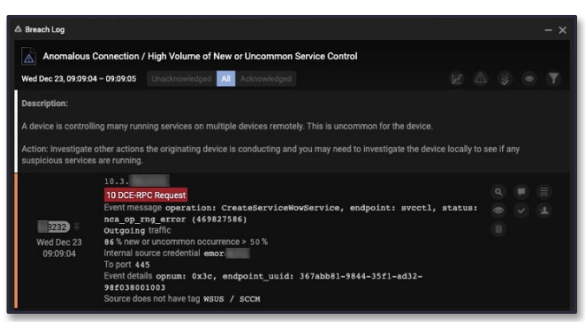

Figure 3: Example breach showing 10 uncommon service controls

- Device / AT Service Scheduled Task

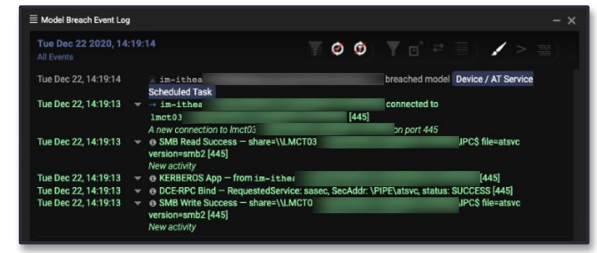

Figure 5: Breach event log shows new AT service scheduled task activity

- Device / Multiple RPC Requests for Unknown Services

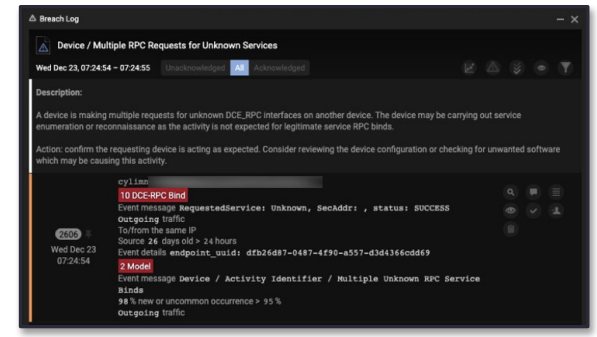

Figure 6: Breach shows multiple binds to unknown RPC services

- Device / Anomalous SMB Followed By Multiple Model Breaches

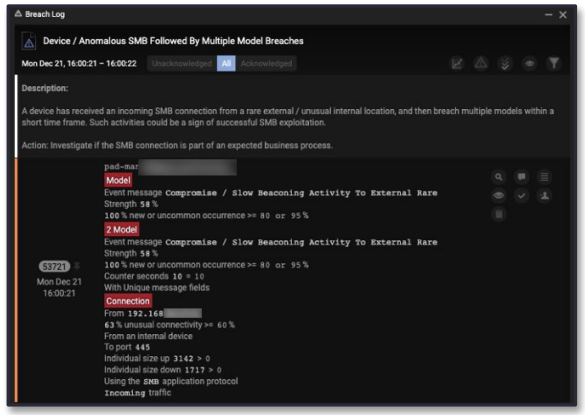

Figure 7: Breach shows unusual SMB activity, combined with slow beaconing

- Device / Suspicious File Writes to Multiple Hidden SMB Shares

Figure 8: Breach shows device writing .bat file to temp folder on another device

- Unusual Activity / Anomalous SMB to New or Unusual Locations

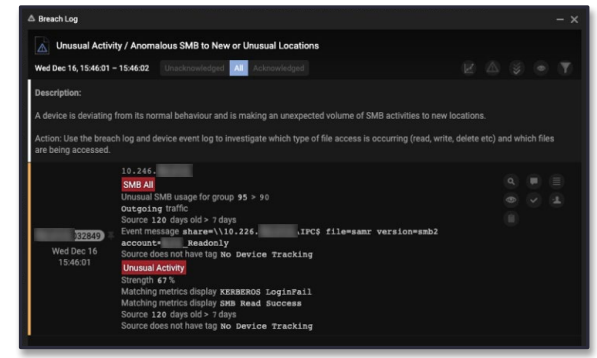

Figure 9: Breach shows new access to SAMR, combined with SMB Reads and Kerberos login failures

- Unusual Activity / Sustained Anomalous SMB Activity

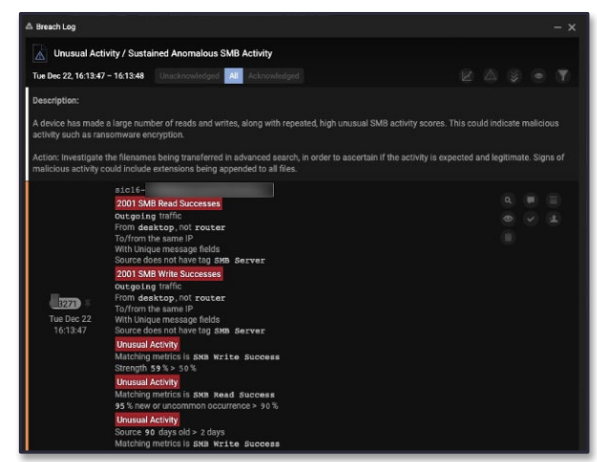

Figure 10: Breach shows significant deviation in SMB activity from device

The Advantage of AI

By understanding where credentials are used and which devices talk to each other, Cyber AI has an unprecedented and dynamic understanding of business systems. This empowers it to alert security teams to enterprise changes that could indicate cyber risk in real time.

These alerts demonstrate how AI learns 'normal' for the unique digital environment surrounding it and then alerts operators to deviations, including those that are directly relevant to the SUNBURST compromise. It further provides insights into how the attacker exploited those networks that did not have the appropriate visibility and detection capabilities.

On top of these alerts, Cyber AI Analyst will also be automatically correlating these detections over time to identify patterns, generating comprehensive and intuitive incident summaries, and significantly reducing triage time. Reviewing Cyber AI Analyst alerts should be given high priority over the next several weeks.

Author Biography

Max Heinemeyer is a cyber security expert with over nine years' experience in the field, specializing in network monitoring and offensive security. At Darktrace, Max works with strategic customers to help them investigate and respond to threats, as well as overseeing the cyber security analyst team in the Cambridge UK headquarters. Prior to his current role, Max led the Threat and Vulnerability Management department for Hewlett-Packard in Central Europe. In this role he worked as a white hat hacker, leading penetration tests and red team engagements. He was also part of the German Chaos Computer Club when he was still living in Germany. Max holds a MSc from the University of Duisburg-Essen and a BSc from the Cooperative State University Stuttgart in International Business Information Systems.

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,500 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

For more information

- Visit darktrace.com
- Book a demo
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn