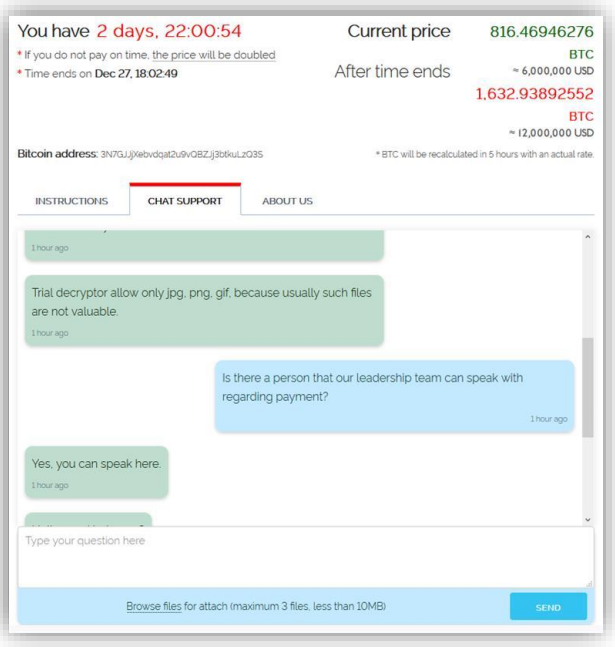
December 23, 2019 Security Incident

Internal Investigation Summary

The purpose of this report is to document the findings of the MSSP internal investigation that was conducted following the security incident that began on December 23, 2109 at 10:42 pm *PST. Findings concluded by a third-party investigation (currently underway by Kroll Services), will provide corroborating evidence to support our internal findings, as well as contribute to our overall action plan as we move beyond remediation and into an improved state of service.

**All stated times are expressed in Pacific Standard Time.*

Executive Summary



According to a ticket logged at 10:42 pm, on December 23, 2019, an MSSP security engineers filed a LogicMonitor Alert that reported Trend Micro Worry-Free Services were deactivated (T20191223.1191), using stolen system credentials. In part of a combined effort, nefarious actors were able to deploy through the an MSSP remote management system (Datto RMM), a malicious payload that encrypted a portion of the an MSSP computing infrastructure (i.e., “Sodinokibi”), including 258 customers and 9,860 machines. an MSSP’s first action was to contain, remediate and clean the impacted devices. an MSSP identified the point of origin and contained the malicious software. This incident resulted from compromised user credentials.

Within one hour of the ransomware being deployed, Security, Engineering and Support Teams were actively engaged in identifying, containing and planning to mitigate the ransomware. By noon on December 24, an MSSP had restored most of its critical infrastructure systems and proceeded to restore customer sites on a case-by-case basis.

Further to restoration efforts, an MSSP secured outside services through Kroll/Red Canary to assist in systemwide forensic analysis to determine cause and effect of the ransomware event. Given that Kroll had, over the course of the past year, investigated more than 100 ransomware events relating to the Sodinokibi variant, a workplan was established between Kroll and an MSSP's Security Core Team and follow-up remediation began with round-the-clock monitoring, event identification, remediation, and daily stand-up reporting on progress.

Security Incident Response Teams Assembled

Within 50 minutes of the event being noted in the system, an MSSP COO, John Frazier, was notified and engaged. Additional resources were assembled according to need, roles and responsibilities.

Multiple Incident Response Teams were assembled over the course of the next 24 hours, and three separate conference bridges were established to support containment and remediation efforts. Approximately 144 employees from within all groups participated in the various responses processes, providing 24-hour support, with most of the teams working an average of 16- to 18-hour shifts, beginning 12/23/2019.

Under CEO's Direction

- 12/24/2019 | 10:40 am – Third-party negotiator agency ("Coveware") engaged to assist. Negotiations with the attackers began to obtain the decryption application. Guidance and updated information was provided throughout the process by Tim Jones and Bill Snow of WhiteDove.
    - Mike Smith—First contact with ransomware perpetrators.
    - Vanessa Johnson—General Counsel, assisted in negotiations between an MSSP, WhiteDove & Sodinokibi ransomware group.

Under COO's Direction

- Josh Black directed the Critical Incident Management Bridge
- Andrew Smith directed the incident bridge with Trend Micro Support (initiated at 01:04 AM PST)
- Dana Johnson directed the incident bridge with Minerva Support (initiated at 02:19 AM PST)

Under CISO's Direction

- Establishment of three separate security teams:

    - 12/24/2019 | 8:30 am – ***Core Security Team***
      This team was responsible for first-contact analysis and review of security controls as they were presently deployed in the an MSSP environment. Additional controls were deployed in cooperation with an MSSP partner, Mindcraft, under the auspices of Mindcraft CEO Eddy Bobsky. Analysis began to be compiled on the current state of the an MSSP computing environment (as far as it could be evaluated with the tools as they were deployed).

        - Drew Williams—Direction, Coordination, Analysis, Reporting
        - Dana Johnson —Deployment, Operational Review, Analysis
        - Josh Black —Forensic Analysis, Operational Support

      After careful review of the situation and understanding the configuration landscape of our corporate infrastructure (and how we serve our clients), an action plan was formulated based on an earlier published document that described a step-by-step contingency.

    - 12/24/2019 | 9:00 am – ***Security Services Support Team***
      This team was comprised of a group of an MSSP engineers and resources to manage current business affairs relative to Security Services as currently stipulated. Coordination between an MSSP security vendor-partners was also coordinated through this group, through which additional resources and post-event planning around critical care and further deployment of tools were being coordinated.

        - Drew Williams—Executive Sponsorship, Initial Vendor Contact
            - SPLUNK—SIEM / SOC Services
            - Rapid7—Vulnerability Management / Assessment Scanning
            - DarkTrace—Anomaly Detection (although not deployed)
            - DATTO—Coordination with CISO for follow-up & Log Analysis
        - Ryan Blue—Security Services Team Management, Project Coordination
            - Minerva—Upgrades & Extended Deployment
            - Trend Micro—Coordinate with internal teams to reactivate
            - DarkTrace—Coordinate on postponing PoV engagements
        - Shawn Boles—Client Security Services Follow-up
            - Cisco—Coordinate SIEM activity
              (limited log analysis was available)
            - Establish the Security Triage & Recovery Bridge for Internal an MSSP Security Team & invited engineers
        - Andrew Smith —Trend Security Controls, Tools Deployment

- 12/26/2019 | 09:00 am – ***Security Core Architecture Team ("SeCAT")***
  A hybrid Team assembled largely based on prior experience with access control, system architecture and security management. Given that this team had already begun work on a contingency plan based on an earlier "test scenario" (coincidently, initiated by a call from CEO to CISO on a client that was facing a ransomware attack), this team had already begun containing and managing the reconfiguration of mission-critical systems, including review and revision of domain controllers to a tighter level of "Least Privilege," and integration/distribution of key security processes and controls.

  - Drew Williams—Executive oversight, MFA planning/coordination, authorization of purchase of Active Directory Plus for immediate distribution and critical care
  - Todd Bland—Infrastructure Architecture, Domain Controller Reconfiguration, Operational Analysis, Access Control Oversight, acquisition of AD+
  - Stephanie Taylor—Identity & Access Management Oversight, Initiation of Mandatory two-factor authentication, Reconfiguration of assets behind 2FA rules
  - Josh Brown—Oversight/coordination of decommissioning all legacy an MSSP VPN's, enforcing all VPN access through next generation Fortinet "Corporate" VPN (internal designation), IAM Oversight & Coordination with other teams
  - Matt Smythe—Assist in domain controller reconfiguration, deployment of AD+
  - Dana Johnson —Security Architecture, Operational coordination, log analysis.

<u>Under COE's Direction</u>

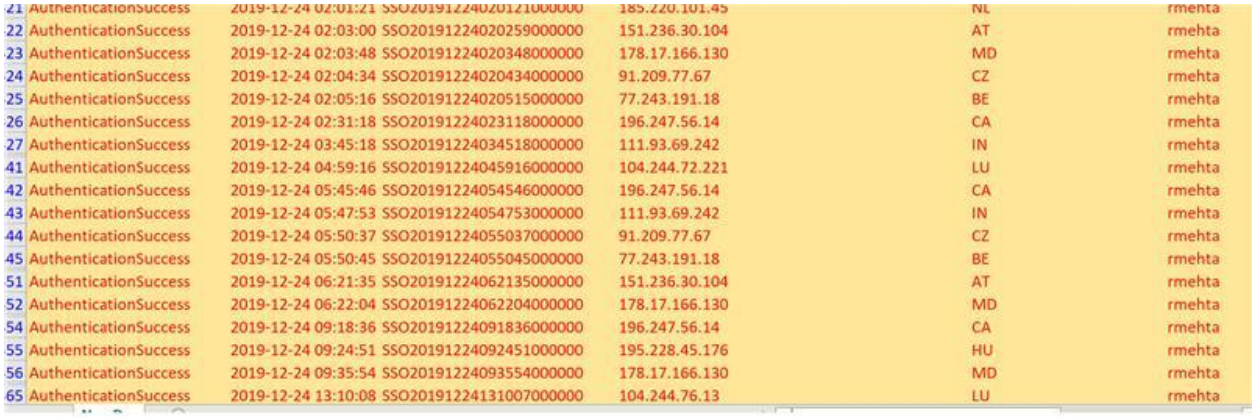
- Establishment of multiple support bridges:

  - 12/24/2019 | 02:00 am – ***COE/Support Ops Critical Incident Management***
    Stephen Currie, VP COE, establishes communications bridge to manage CIM activities, notify and respond to customer queries, restoration of services and remediation of malware deployment using a proprietary key.
    - Todd Bland —Executive oversight, coordination, resourcing
    - Stephanie Taylor —support leadership, coordination, resourcing
    - Andrew Smith—Trend Account Management/Governance
    - Josh Brown —Distribution of decryption scripting
    - Others as directed

NOTE: Additional resources came into activity as they were notified, made aware or returned from holidays.

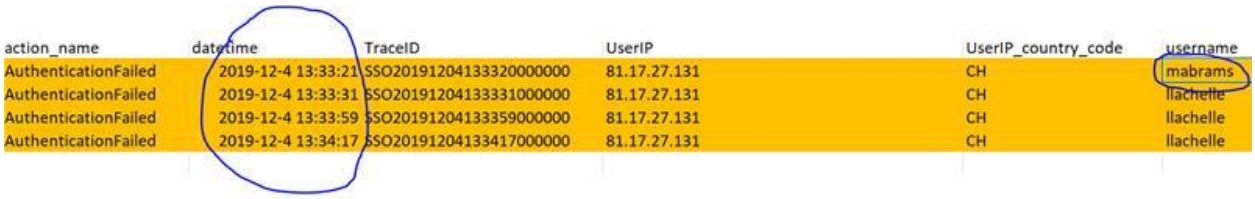
Investigation Approach & Research

1. **Compromised Accounts Identified / Disabled**
   Based on a careful review of audit logs, the following three accounts are identified as having been compromised:
   - Rmehta
     Used to disable Trend Micro Worry Free across all provisioned customers. three specific jobs were established to be executed by malicious code (through the use of three sets of authenticated credentials.



21	AuthenticationSuccess	2019-12-24 02:01:21	SSO2019122402012100000	185.220.101.45	NL	rmehta
22	AuthenticationSuccess	2019-12-24 02:03:00	SSO2019122402025900000	151.236.30.104	AT	rmehta
23	AuthenticationSuccess	2019-12-24 02:03:48	SSO2019122402034800000	178.17.166.130	MD	rmehta
24	AuthenticationSuccess	2019-12-24 02:04:34	SSO2019122402043400000	91.209.77.67	CZ	rmehta
25	AuthenticationSuccess	2019-12-24 02:05:16	SSO2019122402051500000	77.243.191.18	BE	rmehta
26	AuthenticationSuccess	2019-12-24 02:31:18	SSO2019122402311800000	196.247.56.14	CA	rmehta
27	AuthenticationSuccess	2019-12-24 03:45:18	SSO2019122403451800000	111.93.69.242	IN	rmehta
41	AuthenticationSuccess	2019-12-24 04:59:16	SSO2019122404591600000	104.244.72.221	LU	rmehta
42	AuthenticationSuccess	2019-12-24 05:45:46	SSO2019122405454600000	196.247.56.14	CA	rmehta
43	AuthenticationSuccess	2019-12-24 05:47:53	SSO2019122405475300000	111.93.69.242	IN	rmehta
44	AuthenticationSuccess	2019-12-24 05:50:37	SSO2019122405503700000	91.209.77.67	CZ	rmehta
45	AuthenticationSuccess	2019-12-24 05:50:45	SSO2019122405504500000	77.243.191.18	BE	rmehta
51	AuthenticationSuccess	2019-12-24 06:21:35	SSO2019122406213500000	151.236.30.104	AT	rmehta
52	AuthenticationSuccess	2019-12-24 06:22:04	SSO2019122406220400000	178.17.166.130	MD	rmehta
54	AuthenticationSuccess	2019-12-24 09:18:36	SSO2019122409183600000	196.247.56.14	CA	rmehta
55	AuthenticationSuccess	2019-12-24 09:24:51	SSO2019122409245100000	195.228.45.176	HU	rmehta
56	AuthenticationSuccess	2019-12-24 09:35:54	SSO2019122409355400000	178.17.166.130	MD	rmehta
65	AuthenticationSuccess	2019-12-24 13:10:08	SSO2019122413100700000	104.244.76.13	LU	rmehta

   - MAbrams
     Used to deploy scheduled job(s) in Datto RMM. This user account was able to use 2FA using email. This has been validated via O365, DRMM, and Okta logs. Datto RMM account was disabled immediately upon reviewing Datto RMM logs to determine the account used to deploy jobs.



action_name	datetime	TraceID	UserIP	UserIP_country_code	username
AuthenticationFailed	2019-12-4 13:33:21	SSO20191204133320000000	81.17.27.131	CH	mabrams
AuthenticationFailed	2019-12-4 13:33:31	SSO20191204133331000000	81.17.27.131	CH	llachelle
AuthenticationFailed	2019-12-4 13:33:59	SSO20191204133359000000	81.17.27.131	CH	llachelle
AuthenticationFailed	2019-12-4 13:34:17	SSO20191204133417000000	81.17.27.131	CH	llachelle

   - LLaChelle
     Used to deploy unauthorized scheduled jobs in Datto RMM.

2. **Identification, Analysis of Hostile Commands**
   There were three specific scheduled jobs that were setup by the perpetrators

   Scheduled Job #1
   Name: “Updatav2”
   Execution time: 12/23/2019 at 22:56:02 *PST*

Scheduled Job #2
Name: "Updater"
Execution time: 12/23/2019 23:02:21 *PST*

Scheduled Job #3
Name: "Genoa"
Execution time: 12/23/2019 23:11:48 *PST*

- Scope: Targeted 300 of 391 sites available in the NoSecRegulations RMM Role held by mabrams

NOTE: Customers provisioned under both CJIS and ITAR were not impacted as the compromised user account used to create and execute these scheduled jobs (mabrams) did not have access to the Datto RMM sites.

3. Rogue / Hostile IP Addresses Identified, validated

Four identified unique source IP's were identified as being used by perpetrators, and were validated by a task force established by Homeland Security for the purpose of investigating the Sodinokibi ransomware variant. IP addresses were verified as source in review by MSSP's SIEM analysis of logs provided.

- 18.85.192.253
- 79.141.128.99
- 84.16.240.79
- 91.209.77.67

4. Extended application of Critical Care / Limited Compensating Controls

4.1. **Minerva**

The Minerva anti-evasion application became the focal point of compensating controls for immediate defense in the MSSP environment. Minerva was upgraded with additional modules and pushed to a limited range of the MSSP sites and three key customers. In a number of cases, Minerva did prevent the ransomware attack. But, due to exclusions to center-stage RMM (in such case Minerva doesn't protect it and it spawned child processes) the ransomware executed successfully.

- Teams deployed a vaccine (mutex) of the malware to prevent future encryptions, however, findings indicate that beyond its initial (pilot-test), deployment, the Minerva *Ransomware Protection Module* was not enabled. As a result, the Minerva Restore Utility is ineffective (even if Minerva was installed prior to a ransomware outbreak). This has since been activated for all Minerva Agents.
- In the management console, an unusual amount of exclusions such as, the entire Microsoft office suite, Adobe, Datto, etc., were configured to bypass Minerva. These rules have since been disabled and services ensured they remain active.
- In early December, audit logs indicate Minerva prevented multiple attack attempts that are similar to the first stage of the Sodinokibi ransomware.

- During this event, Minerva documented additional (prevented), attempts of evasive attack signatures, which were not detectable by Trend Micro, including file-less attacks and credential harvesting (that is part of larger attack that include lateral movement).
- As part of its scanning protocols, Minerva discovered that on 123 endpoints, the Trend AV application was not running the most current version or was missing altogether.
- Additional analysis revealed that about 1,000 endpoints were configured in "monitor only" mode – which is not "prevention mode."
    - With approval by the Core Security Team, Minerva transitioned those 1,000 endpoints to "full simulation" which is prevention mode.
- Ongoing monitoring has revealed additional nefarious activity:
    - 

    - The events on our console are those that Minerva further prevented. However, because of multiple events of this nature, further analysis has identified that there are endpoints that may still be exposed to compromise.
    - Further analysis from the 2018 Annual Report offered by Minerva revealed that the tool prevented more than 1,500 infection attempts in an MSSP environments.
    - Attacks include multiple strains of high-risk threats and different adware and potentially unwanted programs.
    - Twenty percent of the prevented incidents involved high-risk threats (i.e., Malware classified under this category often include stealthy persistent mechanisms, capability to spread and cause significant losses – either directly (ransomware) or indirectly (stealing financial credentials, destroying an endpoint).
- Access to management console
    - Restricted to mission critical personnel
    - Granted to Minerva Support representatives (Ryan Blue)

4.2. **Trend Micro**

Trend Micro Channel Support assisted an MSSP teams with information gathering related to the unauthorized configuration change. Based on the information available at the time, disabling all but mission critical administration accounts was advised:

- 36 accounts disabled (MSSP personnel)

- 3 account active for operations (Andrew Westfall, Patrick Allen, Steve MacNeil)
- Reference: T20200104.0738

4.3. **Azure AD**

The subscription level at the time of the incident did not allow to gather data for detailed audit log. Alina Sarvey initiated the internal process to upgrade to Azure AD Premium to allow for data retention and Azure AD security features (e.g., visibility into high-risk events)

- 12/28/2019 at 08:08 PM PST Azure AD premium trial activated (T20191228.0729):
  - Trial active for 30 days (ends on 01/27/2020)
  - Includes 100 licenses
  - Upgrade to a paid version will require purchase of Azure Active Directory Premium P2

4.4. Datto PSA and RMM

During the OKTA log review, Security Core Architecture Team identified authentication weakness:

- if a user logins to PSA through Okta or even direct in PSA, some users have an option to open Datto RMM WITHOUT needing to utilize a secondary authentication token (duo, etc.)
- 12/27 12:59 PST: Josh Jones (SCAT) initiated an emergency change request
- 12/27 15:18 PST: Drew Williams approved the change
- 12/27 14:31 PST: Jeff Zweig (admin) implemented the change

5. Response Planning & Contingency Directives

By Christmas morning, our Core Security Team had prepared a defensive and remediation action plan, which included ensuring the MFA test that was implemented in Boise in October was mandated throughout the entire an MSSP infrastructure immediately.

Additional plans as part of a stronger defensive posture included:

- As a cautionary effort, through our SIEM, we are limiting ALL access into/out of the Enterprise to North America and India ONLY and are flagging anything coming from elsewhere as requiring validation.
- From a heightened level of awareness and based on the original access available to the three compromised accounts, we should consider Secret Server as "Compromised" and prepare the appropriate critical care to address this issue.
- We still need to do a full audit of account credentials/activities, which includes ensuring our decommissioning procedures are complete on all counts. It is likely that although two accounts were accessed, there are others with credentials that have been harvested as well (again—for future use).

6. Additional Security Event Monitoring, Review & Analysis

Although we have continued to advance critical care around the MSSP environment, through a series of mission-critical architecture modifications and access controls, given the deployment of our Active Directory + application and additional monitoring capabilities, we are now seeing more events that are considered "at-risk" and require additional investigation:

- At 1:17 PM on 12/26/2019, we saw evidence that there is either another or an extension of the existing compromise underway for specific clients, which we considered a secondary focal point in our urgent incident response proceedings. This led to Stratozen ingesting audit logs that were available from the Datto RMM, which were analyzed, and which validated the three stolen credentials being tied to known hostile IP addresses.
- A number of St John machines (including 10.19.1230.50), are making connections to a proxy avoidance system (tunneling to avoid the firewalls) at 46.101.215.156.
- While this may be appropriate for personal devices on non-work networks, it is not appropriate for devices that are connected to the MSSP Enterprise.
- Audit logs collected at 9:10 PM 01/04/2020 indicate these machines are also trying to gain access to known hostile sites ("hidemyass.com" & "filterbypass.me").

7. Post-event Analysis of Sodinokibi Malware (within the MSSP environment)

7.1. CylancePROTECT

Blackberry Cylance platform is one of the solutions included Endpoint Protection as a Service (EPaaS) portfolio. For the testing purposes, the pilot instance was deployed within the MSSP network in October 2018, and referred as MSSP an MSSP - NFR Partner Lab.

7.1.1. Important notes:

- The pilot group includes 2 actual an MSSP users and their an MSSP issued workstations for the control group – in addition to the lab environment endpoints built specifically for the testing
- Only 1 of these systems was successfully communicating to the Cylance server (SYN-004055, Justin Boot)

7.1.2. Threat Details for SYN-004055 (T20200105.0074):

- Endpoint Details: Windows 10 Pro, CylancePROTECT and Cylance-OPTICS installed on 10/30/2018 (Base Policy : Monitor with Basic Protection applied), reported user an MSSP\jboot
- Malware – Ransom threat event detected and files quarantined on 12/24/2019 at 08:22 AM PST
- Target file info
  - Category: File
  - Detected by: Execution Control
  - File name: javasvc.exe
  - Size: 533.58 KB
  - Path: C:\ProgramData\CentraStage\Packages\20241c4c-d4ea-4376-8463-e38d1a799ed1#**\javasvc.exe**
  - SHA256 hash: 60F1FC7E684C71E0203D7E6EA7FCB691B5CD723A7DA6EF4E4E462AE7F262E857 – associated with Sodinokibi, also called Revil ransomware-type malware

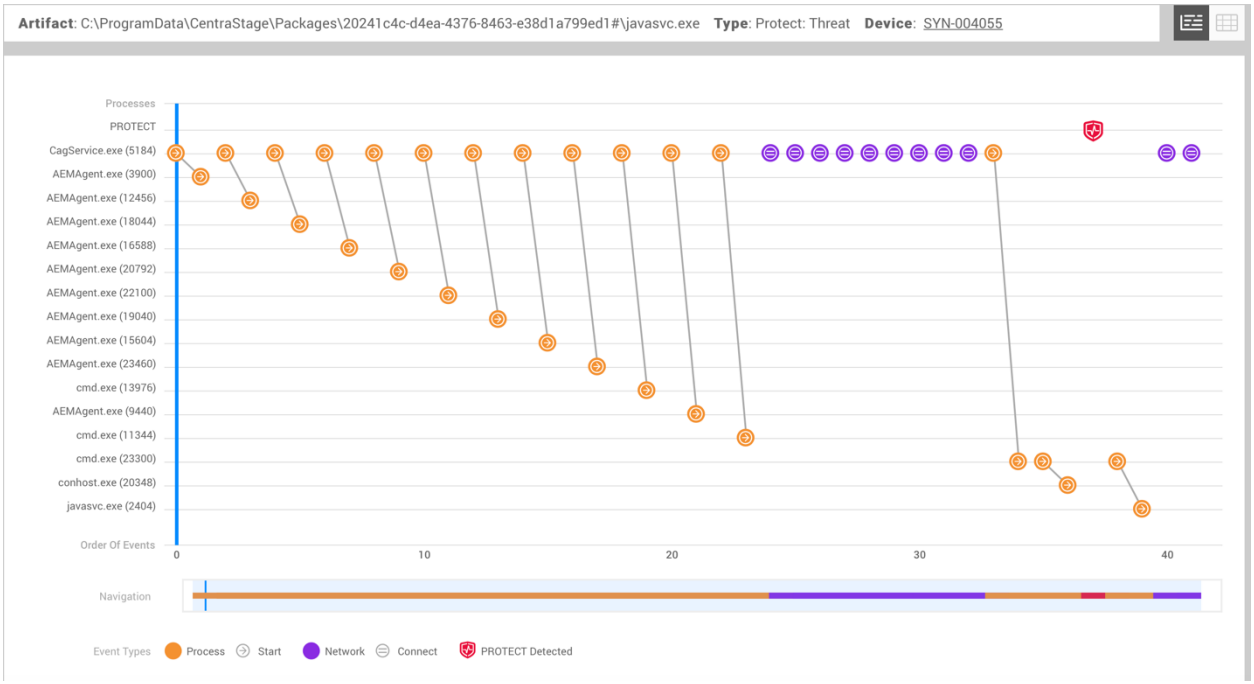


Figure 1 Root Cause Analysis – Cylance-OPTICS

7.1.3. Overview

Sodinokibi, also called Revil is a dangerous ransomware-type malware. Among other tools, it uses advanced encryption techniques and can operate without connection to control servers. Sodinokibi is among the most complex Ransomware in the world.

Origin: ex-USSR

First seen: 4/1/2019

Sodinokibi ransomware is capable of encrypting files with curve25519/Salsa20 and encrypting keys with curve25519/AES-256-CTR. The malware uses 2 public keys to encrypt the private key of the user. In addition, this virus utilizes command and control server obfuscation and can operate using the asymmetric key scheduling algorithm, which allows the malware to function without connection to the C2.

7.1.4. Execution process:

At the beginning of the execution process, the malware generates a mutex which has a hardcoded name. Then, it decrypts a configuration which is embedded. At this stage, Sodinokibi tries to get system privileges by exploiting CVE-2018-8453. With some cases, this step can be omitted in configuration or may not be successful. Then, it tries to obtain privileges by running as an admin.

Following the privilege escalation stage, the ransomware collects basic system and user data. If it finds that the UI or keyboard layout is set to one of the pre-programmed languages, the execution will be terminated. Many of these languages originate from post-USSR territories which may suggest that the malware authors also come from ex-USSR lands.

In a case when the target PC lacks the specified UX or keyboard layout languages, the virus terminates processes by PRC value and proceeds to erase shadow copies. At this point, the data encryption process begins. The ransomware encrypts all user files unless some exceptions are found in the configuration. This is where an attacker can customize their campaign. An extension is then added to all encrypted documents and a README text is placed in directories. The wallpaper is changed to the ransom demand message.

The contents of the ransom note and the README file can be customized by the attackers in the config file which, once again, provides the malware with flexibility which allows it to operate as ransomware-as-a-service since different attackers can demand ransoms of various sums and provide custom instructions to victims.

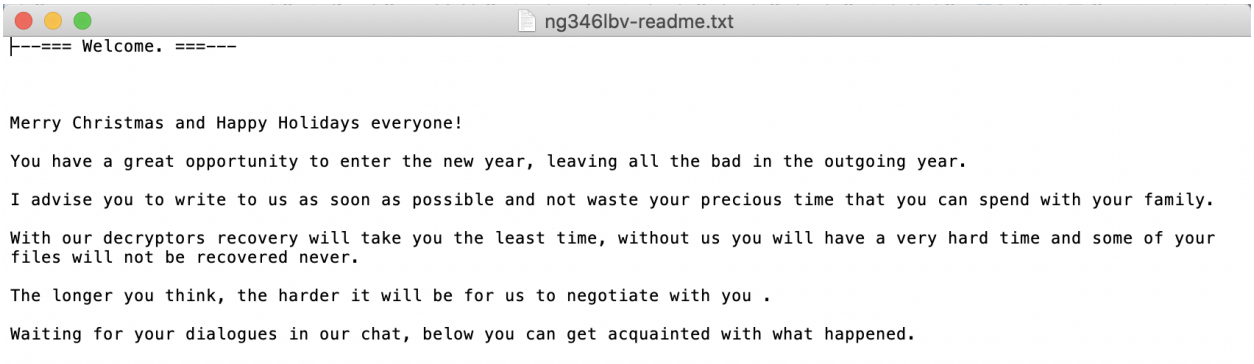


Figure 2 Sample of a README text placed on the Desktop

7.1.5. How does Sodinokibi spread?

To infiltrate the machines of its victims, Sodinokibi takes advantage of quite a number of infection vectors, most of which are very similar to its predecessor - GandCrab. As such, it is known to utilize the CVE-2019-2725 vulnerability and use the RIG exploit kit. Additional, Sodinokibi also spreads via compromised managed service providers. And, like an icing on the cake, on top of the attack vectors mentioned above, this ransomware is often distributed in malicious spam campaigns.

Miscellaneous Notes

Based on a claim posted shortly after the attack, the initial infection vector used by the threat actor was likely a phishing email containing a malicious link (as early as July).

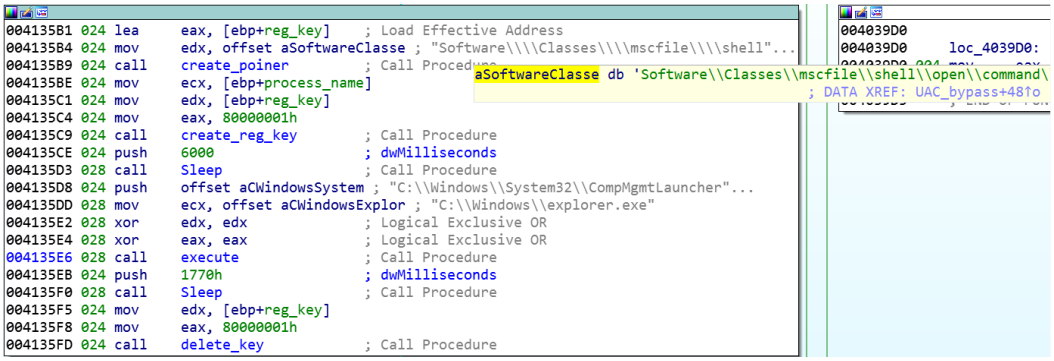
When pressed, the link downloads a *supposedly* legitimate zip file that is actually malicious. Sodinokibi zip files have a very low detection rate on VirusTotal, which signals that the majority of antivirus vendors do not flag the initial payload as malicious. Since the initial Sodinokibi payload is able to pass undetected, the first layer of defense for many organizations is immediately bypassed.

The code responsible for running the exploit first checks if the September 11, 2018 patch (KB4457138) is applied on the machine. This patch addresses multiple vulnerabilities mentioned below. If the patch is not detected, the ransomware proceeds to execute a 32- or 64-bit version of the shellcode depending on the platform architecture. We believe it tries to elevate its privilege by exploiting CVE-2018-8440.

If the system is not vulnerable and the process is still running as a limited user, it will use a RUNAS command to launch another instance with administrative rights and terminate the current instance if it is running with limited privileges.

The module loaded into memory functions as a loader for the next phase of the malware. The module uses *CheckTokenMembership* to confirm the processes' privileges.

If the processes' privileges are insufficient, it tries to bypass User Access Control (UAC). In order to bypass UAC, the malware writes itself to the registry key Software\Classes\mscfile\shell\open\command\ and launches a new instance of explorer.exe to execute CompMgmtLauncher.exe.



When CompMgmtLauncher.exe is executed, it executes anything configured in the registry key Software\Classes\mscfile\shell\open\command\. In this instance, it is executing the

same PowerShell command executed earlier to replace exclamation marks and execute the PowerShell script, but with higher privileges.

The portable executable in memory is the second loader module that will be used for the final payload. In this phase, the malware attempts to inject the ransomware payload into an Ahnlab antivirus process.

In order to do so, the second loader checks to see if Ahnlab antivirus is installed on the target machine. If the Ahnlab V3 Lite software service V3 Service exists, it checks if the file autoup.exe is available. autoup.exe is part of the Ahnlab Updater and is vulnerable to attack.

If the malware is able to find the Ahnlab service and executable, the loader automatically launches the autoup.exe process in a suspended state and attempts to inject the Sodinokibi payload into it via process hollowing.

If the Ahnlab antivirus is not installed on the machine, the loader will launch a separate instance of the current PowerShell process in a suspended state and try to inject the Sodinokibi payload into it via process hollowing. The payload is stored in the module resources as an xor-encrypted portable executable with key 7B.

After the malware encrypts the files on the target machine, it tries to establish communication with a C2 server. In order to generate the URL for the C2, it iterates through a list of domains configured in the previously decoded configuration file.

Sodinokibi Indicators of Compromise

Java Script

- MD5 - 3e974b7347d347ae31c1b11c05a667e2
- SHA1 - 2cc597d6bffda9ef6b42fed84f7a20f6f52c4756

Jurhrtcbvj.tmp

- MD5 - e402d34e8d0f14037769294a15060508
- SHA1 - b751d0d722d3c602bcc33be1d62b1ba2b0910e03

Test.dll

- MD5 - 8ea320dff9ef835269c0355ca6850b33
- SHA1 - f9df190a616653e2e1869d82abd4f212320e9f4b

sodinokibi_loader_1.dll

- MD5 - 7d4c2211f3279201599f9138d6b61162
- SHA1 - ee410f1d10edc70f8de3b27907fc10fa341f620a

sodinokibi_loader_2.dll

- MD5 - 613dc98a6cf34b20528183fbcc78a8ee
- SHA1 - 5cd8eadcd70b89f6963cbd852c056195a17d0ce2

sodinokibi_payload.exe

- MD5 - b488bdeeaeda94a273e4746db0082841
- SHA1 - 5dac89d5ecc2794b3fc084416a78c965c2be0d2a

12/23/2019 11:37 PM Is this really the time?
MSSPsecurity controls were disabled and malicious payload was deployed via our remote management system. How was this done? Can this be done from the RMM? Is the Trend console accessed through a public URL or does it reside on our network? This is a big question here and I do not understand how this was done.

- When we saw this, what actions were taken and by who?

  11:42 PM PST Bridge opened, invitation sent to DL-MS-Priority One

- I heard that Trend was reactived? If so, when and by whom?
  12/24 01:04 AM PST Andrew Westfall directed the incident bridge with Trend Micro Support. Trend Micro Support re-enabled policies during the bridge.
- Was the system then deactivated again? What time and under what user login?
- Please add the data from trend logs to appendix.

12/24/2019 03:13 AM
MSSPcustomers began receiving notice of the ransomware incident via Everbridge communications channels. What an MSSP customers? All customers? A subset of customers? How do we determine what customers are added to everbridge? Did all impacted customers receive these customers?

- When was Coveware engaged?
- When did we notify our insurance agent and who notified them?

10:00 AM
MSSPbegan decrypting locked systems with proprietary algorithm secured through negotiation. (I do not think this is correct. This started on 12/25)

When was Coveware engaged? Why is this not mentioned? What were their findings/observations? Did you talk to them?

Noon
MSSPsecurity controls were reenabled (What specific security controls? When and how?, was AV off the whole time? Why was it not turned on earlier? When and how did we secure the trend console?) and additional critical care began being extended into the an MSSP environment via Minerva anti evasion modules.

1:00 PM
Key internal accounts relating to an MSSP operations were decrypted and restored. What does this mean? Do you mean devices?

4:00 PM
MSSPsecurity processes included initial efforts in notifying and restoring customer infrastructures and accessibility, expanding customer dialog, notifying authorities, and establishment of post-event analysis for forensics purposes.

12/25/2019 01:00 AM -- Ongoing
MSSPSupport and Engineering teams expended our resources to support efforts in notifying and restoring customer access, accounts and activities through decrypt/remediation process scripts.

24-hour communication bridges were established for Security, Support and Architecture teams to coordinate internal efforts with client-facing notifications.

MSSPLeadership begin fielding direct customer calls. (this actually started 12/24). What was the first call? With who? What information was used?

05:18 AM – Attacker impersonates Matthew Abrams in Client Support Bridge | Internal only teams chat

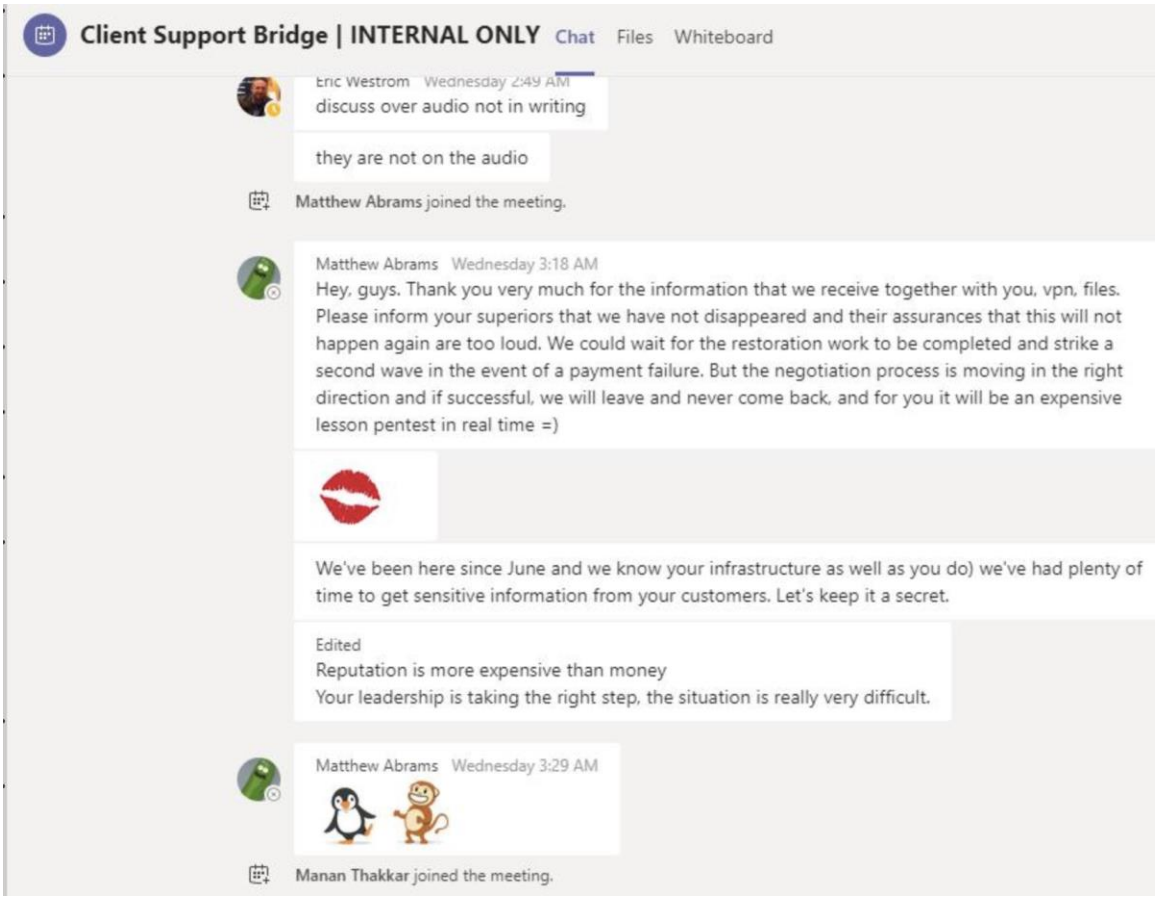


Figure 3 Screenshot take off Teams - MST

12/26/2019 02:00 AM
MSSPbegan mass-deployment of decryption countermeasures to compromised accounts, using a restored (and secure) remote management system. This actually started on 12/25 I believe. What is the basis for your timing here?

10:00 AM
MSSPCore Security Architecture Team began reconfiguring mission-critical systems (including servers and domain controllers) What specifically was changed and why? What security activities/investigation led to this?

12/27/2019 11:00 AM
MSSPengaged third-party Forensics agency, Kroll/Red Canary, and began deploying additional security controls throughout its infrastructure for forensics analysis and system hardening.

As part of an overall effort to focus critical control around the MSSP environment, all links between auto-authentication and the an MSSP remote management systems were disconnected.

12/28/2019 01:00 AM – Ongoing
MSSPSupport and Engineering teams continue to work on customer restoration while security engineers and the Core Security Architecture Team continue work on review and revisions to all mandatory Two-factor Authentication protocols, which include reconfiguration of critical domain controllers.
This is also mentioned as having happened on 12/26? What was done on 12/28.

12/29/2019 **01/03/2020** (Ongoing)

Work continues as it pertains to identifying compromised systems, at which point systems are either replaced or remediated with the proprietary decryption code. Follow-up review of potential risk of residual "bad code" is assessed as well, at which point there has been no indication of such code or additional activity beyond the initial deployment of the ransomware. Does this mean we have not identified all compromised systems? Seems hard to say it is contained if we are still identifying. ????

Conclusions & Analysis

- Although the account that was accessed to gain control of the RMM system and disable an MSSP's security controls, was deactivated (does Matt Abrams have access today?), additional critical analysis is currently underway. What does this mean? In one of your communications, you stated 3 accounts were compromised. What was the basis for this statement?
- Root cause of entry and potential assessment of additional Indicators of Compromise are also being reviewed as part of our ongoing assessment and forensic analysis. This is meaningless. This seems pretty easy to figure out. What were your findings?

- The accounts identified as “Compromised” as part of this event were immediately deactivated, and assets isolated for forensic analysis. What assets specifically? an MSSP computer? Home computer? Others? Did we interview person.
- MSSPhas also established a protocol for remediating all impacted devices, which includes restoring from backup or decrypting, scanning each device for malicious executables, and restarting all security services. Good.
- MSSPsecurity architects, analysts and third-party forensics teams are now reviewing the audit logs and residual artifacts associated with the code that was packaged and delivered to certain end-point devices. What logs are being reviewed specifically? Trend logs? Minerva logs? Firewall logs? RMM logs? PSA logs? OKTA logs?
- Based on the findings as they have been reported (as of January 3, 2020), no compromise or indication of exfiltration of Protected Information (i.e., “PII,” “EPHI,” etc.), has been discovered. Seems that way, but what is the basis for that finding?
- All legacy single-point VPNs have been retired from the MSSP environment and all VPN connections have been replaced with next-generation multi-factor VPN connectivity. Good.
- Additional critical care through increased focus on an MSSP edge devices has included deployment of endpoint security monitoring and prevention applications, anti-evasion, and anomaly detection applications.
- A comprehensive root cause analysis and post-event forensic report is expected within the next 10 to 21 days.
- What about multi-factor authentication for accessing RMM?