THE COMPUTER CORNER

No. 237: Hams, Keep Your Eyes and Ears Open

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

This was sent to notify us of "threat actors", who target several infrastructure sectors in the US. I have reprinted only about half of the email, to give you a taste of what it covers. For the entire document, which you should read, go to: https://www.us-cert.gov/ncas/alerts/TA17-293A This is serious stuff, and those of us in the ham community have an obligation to keep alert and notify authorities of suspicious activity. That is all I will say. Read the following and access the TA17-293A document for a complete read.

From: "US-CERT" US-CERT@ncas.us-cert.gov **Date:**20-Oct-17 Friday 10:06 PM
Subject: TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors

U.S. Department of Homeland Security US-CERT National Cyber Awareness System:

Overview: This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on advanced persistent threat (APT) actions targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors. Working with U.S. and international partners, DHS and FBI identified victims in these sectors. This report contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by APT actors on compromised victims' networks.

Description: Since at least May 2017, threat actors have targeted government entities and the energy, water, aviation, nuclear, and critical manufacturing sectors, and, in some cases, have leveraged their capabilities to compromise victims' networks. Historically, cyber threat actors have targeted the energy sector with various results, ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict. [1] Historically, threat actors have also targeted other critical infrastructure sectors with similar campaigns.

Analysis by DHS, FBI, and trusted partners has identified distinct indicators and behaviors related to this activity. Of specific note, the report Dragonfly: Western energy sector targeted by sophisticated attack group, released by Symantec on September 6, 2017, provides additional information about this ongoing campaign. [2]

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks. The initial victims are referred to as "staging targets" throughout this alert. The threat actor uses the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. The ultimate objective of the cyber threat actors is to compromise organizational networks, which are referred throughout this alert as "intended target."

Technical Details

The threat actors in this campaign employed a variety of TTPs, including:

open-source reconnaissance,
spear-phishing emails (from compromised legitimate accounts),
watering-hole domains,
host-based exploitation,
industrial control system (ICS) infrastructure targeting, and
ongoing credential gathering.

Using Cyber Kill Chain for Analysis

DHS leveraged the Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. Phases of the model include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. This section will provide a high-level overview of activity within this framework.

Stage 1: Reconnaissance

The threat actors appear to have deliberately chosen the organizations they targeted, rather than pursuing them as targets of opportunity. Staging targets held preexisting relationships with many of the intended targets. It is known that threat actors are actively accessing publicly available information hosted by organization-monitored networks. DHS further assesses that threat actors are seeking to identify information pertaining to network and organizational design, as well as control system capabilities, within organizations.

Forensic analysis identified that threat actors are conducting open-source reconnaissance of their targets, gathering information posted on company-controlled websites. This is a common tactic for collecting the information needed for targeted spear-phishing attempts. In some cases, information posted to company websites, especially information that may appear to be innocuous, may contain operationally sensitive information. As an example, the threat actors downloaded a small photo from a publicly accessible human resources page. The image, when expanded, was a high-resolution photo that displayed control systems equipment models and status information in the background.

Analysis also revealed that the threat actors used compromised staging target networks to conduct open-source reconnaissance to identify potential targets of interest and intended targets. “Targets of interest” refers to organizations that DHS observed the threat actors showing an active interest in, but where no compromise was reported. Specifically, the threat actors accessed publicly web-based remote access infrastructure such as websites, remote email access portals, and virtual private network (VPN) connections.

Stage 2: Weaponization Spear-Phishing Email TTPs

Throughout the spear-phishing campaign, threat actors used email attachments to leverage legitimate Microsoft Office functions to retrieve a document from a remote server using the Server Message Block (SMB) protocol. As a part of the standard processes executed by Microsoft Word, this request authenticates the client with the server, sending the user’s credential hash to the remote server prior to retrieving the requested file. (Note: It is not necessary for the file to be retrieved for the transfer of credentials to occur.) The threat actors then likely used password-cracking techniques to obtain the plaintext password. Once actors obtain valid credentials, they can masquerade as authorized users.

Stage 3: Delivery

When seeking to compromise the target network, threat actors used a spear-phishing email campaign that differed from previously reported TTPs. The spear-phishing email used a generic contract agreement theme, with the subject line “AGREEMENT & Confidential”, and which contained a generic PDF document, titled “’’document.pdf”. (Note the inclusion of two single apostrophes at the beginning of the attachment name.) The PDF itself was not malicious and did not contain any active code. The document prompted the user to click on a link should a download not automatically begin. (Note: No code within the PDF initiated a download.) The link directs users to a website via a shortened URL, which may prompt them to retrieve a malicious file.

In previous reporting, DHS and FBI identified the common themes used in these spear-phishing emails, all emails referred to control systems or process control systems. The threat actors continue to use these themes, specifically against intended target organizations. Email messages include references to common industrial control equipment and protocols. The emails leveraged malicious Microsoft Word attachments that appear to be legitimate résumés or curricula vitae (CVs) for industrial control systems personnel, as well as invitations and policy documents that entice the user to open the attachment. The list of file names has been published in the IOC.

Stage 4: Exploitation

Threat actors used distinct and unusual TTPs (i.e., successive redirects) in the phishing campaign directed at staging targets. Emails contained a stacked URL-shortening link that directed the user to http://bit[.]ly/2m0x8IH link, which redirected the user to http://tinyurl[.]com/h3sdqck link, which redirected the user to the ultimate destination of http://imageliners[.]com/nitel. The imageliner[.]com website contained an email address and password input fields mimicking a login page for a website.

When exploiting the intended targets, threat actors used malicious .docx files to capture user credentials, however, DHS did not observe the actors establishing persistence on the user’s system. The documents attempt to retrieve a file through a “file:\” connection over SMB using Transmission Control Protocol (TCP) ports 445 or 139 and User Datagram Protocol (UDP) ports 137 or 138. This connection is made to a command and control (C2) server — either a server owned by the threat actors or that of a compromised system owned by a staging location victim. When a user is authenticated as a domain user, this will provide the C2 server with the hash of the victim. Local users will receive a graphical user interface (GUI) prompt to enter a username and password. This information will be provided to the C2 over TCP ports 445 or 139 and UDP ports 137 or 138. (Note: A file transfer is not necessary for a loss of credential information.) Symantec’s report associates this behavior to the Dragonfly threat actors in this campaign. [3]

Use of Watering Hole Domains

One of the threat actors’ primary uses for staging targets is to develop watering holes. The threat actors compromise the infrastructure of trusted organizations to reach intended targets. [4] Although these watering holes may host legitimate content by reputable organizations, the threat actors have altered them to contain and reference malicious content. Approximately half of the known watering holes are trade publications and informational websites related to process control, ICS, or critical infrastructure.

Using a similar SMB collection technique, the actors manipulated these websites by altering JavaScript and PHP files that redirect to an IP address on port 445 for credential harvesting. The compromised sites include both custom developed web applications and template-based frameworks. The threat actors injected a line of code into header.php, a legitimate PHP file that carried out the redirected traffic.

There is no indication that threat actors used zero-day exploits to manipulate the sites; the threat actors more likely used legitimate credentials to access the website content directly.

Now go read the entire document. https://www.us-cert.gov/ncas/alerts/TA17-293A Happy computing!