

MUDCARP'S FOCUS ON SUBMARINE TECHNOLOGIES



TABLE OF CONTENTS

Key Findings.....	3
Technical Mitigations	4
Historical and Related MUDCARP Indicators	11

1. SUMMARY

After an extensive investigation, which revealed a widespread campaign targeting multiple universities, Accenture's iDefense unit is publishing this report to provide threat indicators and mitigation approaches to help organizations defend themselves and ensure cyber resilience against this threat group. It's imperative to highlight the third-party risk and supply chain threat from advanced cyber adversaries. Organizations need to understand that espionage actors will seek to exploit any organization within a target's supply chain to fulfill its strategic collection requirements.

The authors of the technical paper titled "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War"¹ draw attention to the issue of adversarial targeting of the DoD supply chain by stating that most nation states have a full complement of technologies and resources available to achieve their asymmetric strategies and goals as they relate to cyberespionage. They take advantage of the inherent vulnerabilities² in the complex DoD supply chain ecosystem, namely a lack of oversight associated with operational security and siloed threat intelligence sharing.

As referenced in the "Accenture Cyber Threatscape Report 2018,"³ supply chains are integral to the DoD as the Department works to bring its technologies and weapon platforms to maturity. Threat actors have identified these supply chains as effective means of infiltrating victim organizations. Even verticals like aerospace and defense, in which companies have bought into the maintenance of mature security hygiene or in which the regulatory landscape has forced such adoption, supply chains still present openings.

Key Findings

- Based upon tactics, techniques and procedures (TTPs) correlations, campaign targeting, leveraged malware, infrastructure and compelling third-party intelligence,⁴ iDefense analysts have moderate to high confidence that this activity is attributed to the MUDCARP (aka "TEMP.PERISCOPE" and "Leviathan") threat group.
- As referenced in a recent Wall Street Journal article⁵ MUDCARP collection requirements appear to include several very specific submarine technologies produced by multiple cleared defense contractors (and their respective supply chains). Any technology or program that involves the delivery or launching of a payload from a submerged submarine, or undersea autonomous vehicles, is of high interest to MUDCARP.
- It is likely that MUDCARP actors have targeted several cleared defense contractors, universities (both domestic and foreign), and oceanographic institutes.
- MUDCARP and other cyberespionage threat groups will continue to target companies, think tanks and universities who are in the DoD supply chain as a means of stealing intellectual property and exploiting those business relationships targeting DoD organizations.

¹ Gronager, John, et. al. "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." August 2018. Mitre. <https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf>.

² These vulnerabilities could include everything from patch management to employee education and awareness

³ "Cyber Threatscape Report 2018." Accenture. <https://www.accenture.com/us-en/insights/security/cyber-threatscape-report-2018>.

⁴ Henderson, Scott, et. al. "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally." July 10, 2018. FireEye. <https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html>.

⁵ "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets". WSJ <https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800>.

2. MITIGATIONS & RECOMENDATIONS

Organizations can proactively defend against cyberespionage campaigns targeting supply chain assets by enforcing policies and procedures designed to adhere to DoD supply chain requirements and best practices. According to Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012⁶, “Safeguarding Covered Defense Information and Cyber Incident Reporting”, entities which comprise the DoD supply chain, except for contracts solely for the acquisition of commercial off-the-shelf (COTS) items, have had to become National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171⁷ compliant no later than December 31, 2017. This publication, titled “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”, provides recommended security requirements for protecting the confidentiality of controlled unclassified information when such information is resident in nonfederal systems and organizations.

The security requirements contained in SP 800-171 are broken down into fourteen categories or “families” which include access control, configuration management, incident response, and risk assessment among many others. The publication then identifies specific controls, policies, and procedures for each category that relate to the general topic of the family. For example, under Access Control, it is requirement that the supply chain organization authorize remote execution of privileged commands and remote access to security-relevant information. Another example, under the Incident Response family, states that tracking, documenting and reporting incidents to designated officials both internal and external to the targeted organization. iDefense recommends that the requirements outlined in this publication should be immediately implemented and enforced by any company or institution producing goods or services or conducting research on behalf of the DoD. These best practices also advertise that contractors and academic institutions educate their employees as to the breadth, depth and scope of the adversary, and the risks imposed to national security; doing so will help to try to ensure an environment of supplier security and resilience by incentivizing proper security controls and threat intelligence sharing.

Regarding the detection and remediation of MUDCARP campaigns, organizations should focus on educating staff on how to detect socially engineered e-mails and the repercussions of enabling macros in Office documents sent via e-mail. In addition, security professionals should specifically enable alerts to detect tools and techniques frequently utilized by MUDCARP actors. These include the delivery of malicious Microsoft Office documents exploiting the CVE-2017-11882 vulnerability; the use of a custom backdoor written in JavaScript known as “Orz” that retrieves attacker commands from compromised websites and MUDCARP-created profiles on legitimate networking sites; and “China Chopper,” a simple Web shell designed to run on a variety of Web servers that allows an adversary to download files, access the victim system’s Active Directory, and determine passwords via a brute-force attack.

Technical Mitigations

iDefense suggests organizations consider rapidly prioritizing Microsoft Office Suite application patching and updating due its high popularity and constant targeting by threat groups. For example, CVE-2017-8759’s patch was available on September 12, 2018, and MUDCARP was able to deliver weaponized CVE-2017-8759 RTF documents to targets 3 days later. This 72-hour time frame is typically faster than most organizations 30-day Window for patching - leaving them vulnerable to attacks by agile threat groups such as MUDCARP.

iDefense suggests organizations perform management of privileged accounts like the default Administrator account, which should be disabled and removed from systems. Threat actors like MUDCARP often target users with enhanced privileges and those users should adhere to least privilege principals by limiting their use of privileged accounts to mitigate threat actors from exploiting their elevated permissions and authorization by enforcing role-based training and security policies. As an example, some of the malicious MUDCARP samples identified above will not properly execute unless the targeted victim is the Administrator user account when opening the lure documents.

iDefense suggests organizations configure its e-mail gateways to inspect DKIM Signatures, SPF & DMARC records to detect the absence or failure of such identifiers with incoming mail - as these authentication and identification items

⁶ DFARS 252.204-70**. Under Secretary for Acquisition, Technology, and Logistics. <https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>

⁷ NIST Special Publication 800-171. National Institute of Standards and Technology. <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>

have not been typically observed on MUDCARP infrastructure and phishes. If these tests fail, consider appending indicators and warnings (I&Ws) in the e-mail subject line, such as [SUSPICIOUS] or [IDENTITY-UNVERIFIED] in addition to the normal [EXTERNAL] tag for incoming e-mail. Implementation of these I&Ws would additionally need to be followed up with enhanced phishing training for your users to understand what these warning mean, and how it does not positively confirm a malicious e-mail or phish but should alert them to treat the e-mail with caution.

iDefense suggests organizations implement network segmentation, segregation and isolation for research/high-value systems in enclave networks. Threat groups like MUDCARP specifically target intellectual property and research for espionage or theft in these systems. Controlling information boundaries and security perimeters of these high-value/research systems is critical to making them defensible as part of best practices for secure network architecture. It is advisable to request researchers define the operational network requirements (if any) needed for their research & development systems. Once defined, then strictly enforce network access to only permitted and approved destinations to mitigate exposure to threat actor infrastructure, such as MUDCARP standing up brand new domains and IPs as C2s that are not necessary for researchers to connect to perform their work.

iDefense suggests organizations implement Web-proxy interception, categorization, and filtering of Internet-accessible websites. Threat actors like MUDCARP often establish new domains or sites without a visible or functional website that any visitor would find convincing or useful. Web proxies can evaluate these new domains and sites to determine functionality, popularity, newness, and reputation, which are criteria that can be used to block these sites – preventing additional malicious actions or content from being delivered to the targeted user. iDefense suggests reviewing your Web-proxy configuration settings to determine the effects of blocking “uncategorized,” “unpopular,” and “suspicious-” like categories available from your proxy.

iDefense suggests that organizations identify all the user-agents installed within their environment and enforce software-baselines to make it easier for security to identify anomalous or rogue user-agents performing connections to external sites through network interception and monitoring. Threat actors like MUDCARP will sometimes utilize unique User-Agent strings to establish connections, for example: `Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUSMSE` - which can be more easily identified during security monitoring if there is a list of known standardized User-Agents to compare against.

iDefense suggests organizations consider migrating to Windows 10 or newer OS. Threat Actors like MUDCARP can utilize techniques like Reflective DLL Loading to write a DLL into memory and load a shell, like Meterpreter – which gives them backdoor access to the victim. However, Windows 10 OS now has Windows Defender Advanced Threat Protection (ATP), Exploit Guard, and Import Address Table Access Filtering (IAF) which can detect these techniques and upcoming security features that could even potentially mitigate it by requiring files to exist on disk before they can be executed in combination with application-whitelisting.

iDefense suggests that organizations implement PowerShell security features. Threat actors such as MUDCARP are known to utilize PowerShell to issue malicious commands and operate on compromised systems. To mitigate this tactic, enable PowerShell script block logging through the Windows Components -> Windows PowerShell -> "Turn on PowerShell Script Block Logging" policy value option. Furthermore, disable the PowerShell 2.0 version with the command "Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root." In addition, if your staff do not need or use PowerShell for business operations, consider setting the execution policy to be very restrictive all users and monitor for any suspicious use of PowerShell on systems.

iDefense suggests organizations review and test OLE/COM blocking controls in their environment to determine if they can still complete necessary business operations without Object Linking and Embedding (OLE)-embedded functionality. Threat actors like MUDCARP are likely to continue to utilize OLE as a method to insert malicious content inside various phishing documents. OLE/COM component activation can be blocked through the following registry key change: "Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Microsoft\Office\16.0\Common\COM Compatibility\{CLSID} DWORD ActivationFilterOverride = 1".

iDefense suggests as a precaution that your organization configure Microsoft Office applications with secure technical implementations that may mitigate current and future MUDCARP attack techniques that target this suite of software, such as the following:

- Threat actors may attempt to force Office applications to spawn an instance of Internet Explorer that loads dangerous content, such as ActiveX. To mitigate this, enable "Restrict ActiveX Installs" in Internet Explorer, enable "Scripted Window Security Restrictions" and enable Binding of these security policies to Microsoft office applications through the Security Settings -> IE Security "Bind to Object" so they cannot be bypassed.
- Threat actors may embed navigation to URLs or other hyperlinks within lure document to compromise the user. To mitigate this technique, enable the block of URL navigation from Office files through the Security Settings -> IE Security "Navigate URL" option. Furthermore, consider training users to manually navigate in URLs needed for business and to be wary of such links provided by external sources.
- Threat actors may utilize exploits in certain Office documents and templates. Enable Protected View to mitigate exploits for files originating from the internet, files located in potentially unsafe locations and Outlook attachments, through the Security -> Trust Center -> Protected View options. Furthermore, enable Data Execution Prevention (DEP) through the System -> Advanced system settings -> Settings -> Data Execution Prevention -> "Turn on DEP for all programs and services except those I select" option. In addition, enable Control Flow Guard (CFG) through the Windows Defender Security Center -> App & browser control -> Exploit protection settings -> System settings -> "Control flow guard (CFG)" option.
- Threat actors may embed macros or VBA scripts in Office files to execute malicious actions. Block macros from running in Office files from the Internet through the Security -> Trust Center options. Furthermore, disable trusted access to the VBA object model through the Security -> Trust Center "Trust access to Visual Basic Project", disable "VBScript to run in Internet Explorer" and train users to be wary of all macros from external sources.
- Threat actors may establish second-stage payload and malware downloads through the initial e-mail attachment and deceive users or bypass download warning prompts. To mitigate this, disable any file downloads requested by Office applications through the Security Settings -> IE Security "Restrict File Download" option.
- Threats actors may link external content inside Office files which can cause changes in the document without the user's knowledge. To mitigate this, disable automatic updating of links through the Word Options -> Advanced "Update automatic links at Open".
- Threat actors may use password-protection or other rights-management features in Office files to encrypt malicious macros or scripts within the file to bypass Anti-Virus scanning. To mitigate this, enable scanning of encrypted macros through the Security -> Trust Center "Scan encrypted macros in Word Open XML documents" option.
- Threat actors may attempt to load local Web pages through Office files to bypass security controls. To mitigate this, disable local machine zone elevation through the Security Settings -> IE Security "Protection From Zone Elevation" option. Furthermore, block invoked hyperlink instances of popups from Office documents through the Security Settings -> IE Security "Block popups" option.
- Threat actors may attempt to load malicious files through external web content. To mitigate this, enable the Smart Screen Filter through the Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn on SmartScreen Filter scan" option.
- Threat actors may also target wordpad.exe rather than winword.exe with RTF files - so exploit protection mitigations should be enabled to mitigate against this. Enable Control Flow Guard (CFG) through the Windows Defender Security Center -> App & browser control -> Exploit protection settings -> System settings -> "Control flow guard (CFG)" option for wordpad.exe.

iDefense suggests maintaining and configuring any detonation chambers, or anti-malware sandboxes to match the current running configuration and software versions of production systems in your environment. This can be important for running and testing incoming files to your organizations for the presence of malicious code that may only specifically target certain product versions with new vulnerabilities that may not correctly exploit sandboxes that diverge from production.

iDefense suggests that organizations actively hunt for attachments sent to your organization with the presence of OLE-embedded objects, Equation Editor and linked objects. An example of one of these hunting rules is provided below for reference:

```
rule CVE_2017_11882{
  meta:
    description = "Exploit for CVE-2017-11882"
    author = "iDefense Vulnerability Research Labs"
  strings:
    $rtf_header = "\rtf" nocase
    $rtf_objclass = "\objclass" nocase
    $rtf_objupdate = "\objupdate" nocase
    $rtf_objdata = "\objdata" nocase

    $equation_text = "Equation.3"
    $equation_hex = "457175617469666e2e33"
    $ole_header_hex = "d0cf11e0a1b11ae1"

    $text_1 = "636d64" nocase
    $text_2 = "7374617274" nocase
    $text_3 = "6d73687461" nocase
    $text_4 = "68747470" nocase

  condition:
    3 of ($rtf_*) and
    2 of ($text_*) and
    1 of ($equation*) and
    $ole_header_hex
}
```

3. MALWARE ANALYSIS & INDICATORS

The weaponized lure document "Questions about thestory.rtf" emailed to the principal oceanographer in UW's Applied Physics Laboratory is seen below. The table boxes seen on the bottom of page 3 contain the CVE-2017-11882 buffer overflow of the EQNEDT32.EXE component.

File Name: Questions about thestory.rtf

MD5: aca7037286b64b0da05c9708d647c013

SHA1: d84eb5b6c506d22eaf6bcb2b4f743101d010e721

SHA256: c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9

SSDEEP: 1536:rfvBRI3b0NXC7i9NQK+blswpPnzzXTPwsQrQNMovRTnf4u3n:rf5RI3b0NXCuxpPfbQrS

Size (bytes): 88,079

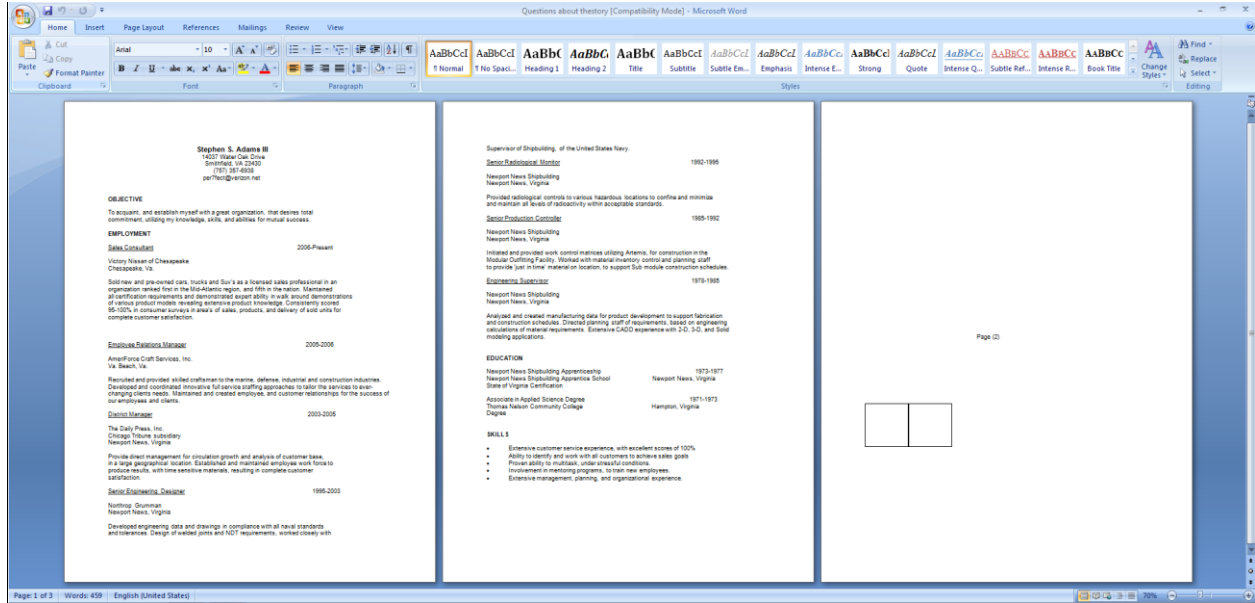


Exhibit 1: Analyst-derived Screenshot of “Questions about thestory.rtf” file in Microsoft Word

The RTF document contains following embedded OLE objects:

Object #1

- Object Size: 25,328
- Object Location: start offset 0000494B - end offset: 00010F2B

Object #2

- Object Size: 9,243
- Object Location: start offset 00010F7B - end offset: 0001580C

Object #1 which is stored as an OLE package, has following metadata:

- Filename = '8.t'
- Size: 25,088
- MD5: A1D5B6E2FD42A90D6225DA28B6B9A70D
- Source path = 'C:\Aaa\tmp\8.t'
- Temp path = 'C:\Users\ADMINI~1\AppData\Local\Temp\8.t'

Object #2 contains a shellcode that exploits 2017-11882 (EQNEDIT).

If the targeted user opens the weaponized document inside a vulnerable version of Microsoft Office and additionally clicks the table shown in Exhibit 1, the weaponized document tries writing “8.t” into following folder and the shellcode within object #2 then tries performing a custom rotating XOR cypher to decode the 8.t file. Exhibit 2 through 5 show screenshots of the XOR cypher routine, pseudo representation of XOR cypher routine, and the decoded “8.t” before and after decryption:

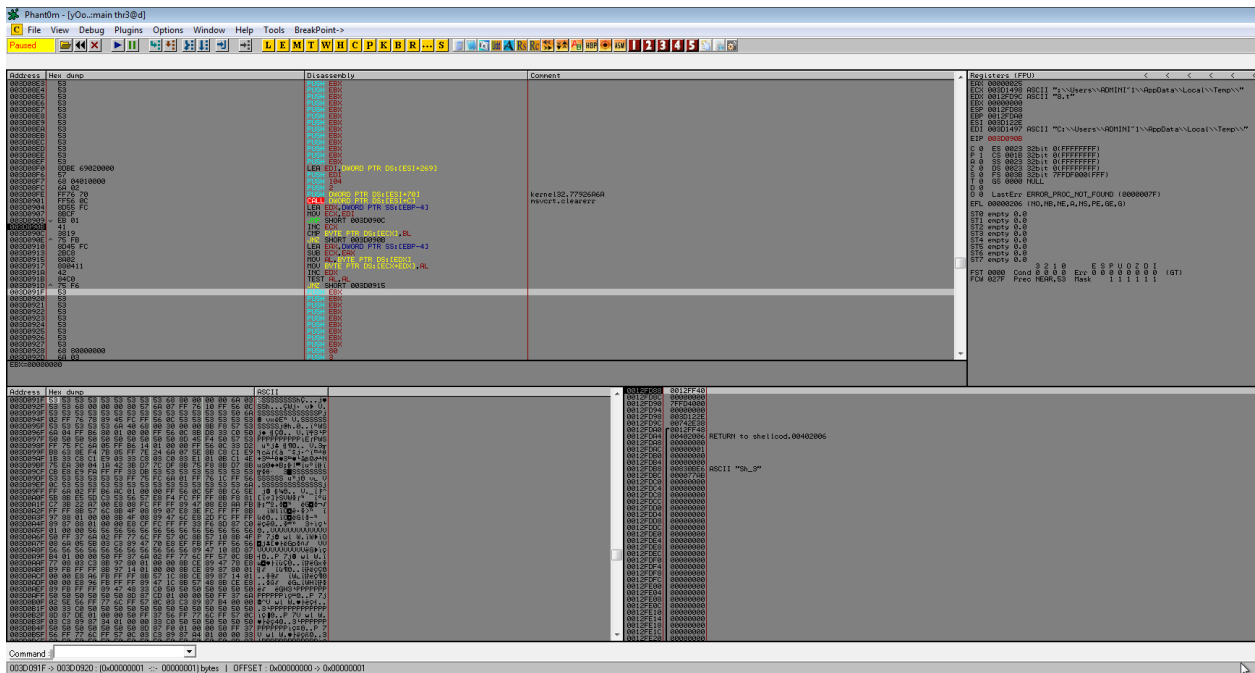


Exhibit 2: Analyst-derived Screenshot of Shellcodeconstructing the 8.t Filename and Location

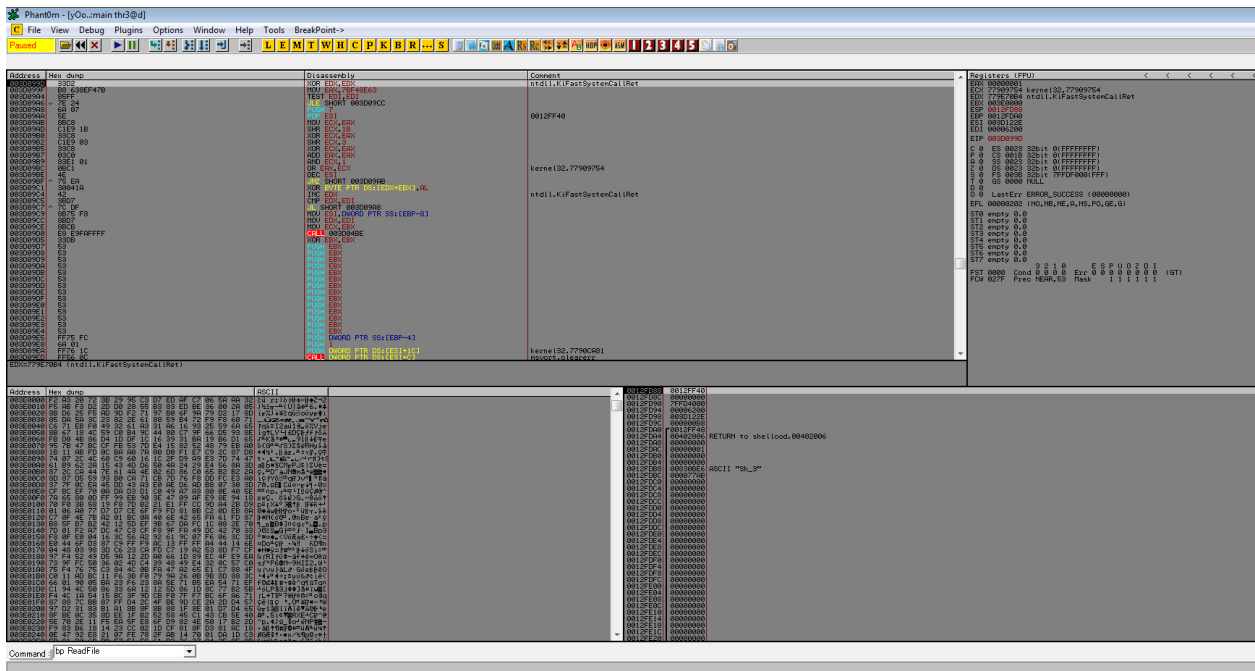


Exhibit 3: Analyst-derived Screenshot of Shellcode loading 8.t Prior to Custom XOR Cypher

```

130 | v10 = 0;
131 | v11 = 0x7BF48E63;
132 | if ( u8 > 0 )
133 | {
134 |     do
135 |     {
136 |         v12 = 7;
137 |         do
138 |         {
139 |             v11 = ((unsigned __int8)v11 ^ (unsigned __int8)((v11 ^ (v11 >> 27)) >> 3)) & 1 | 2 * v11;
140 |             --v12;
141 |         }
142 |         while ( v12 );
143 |         *(_BYTE *)(v10++ + u9) ^= v11;
144 |     }
145 |     while ( v10 < u8 );
146 |     v1 = v15;
147 | }

```

Exhibit 4: Analyst-derived Screenshot of Pseudo Code Representation of Custom XOR Cypher

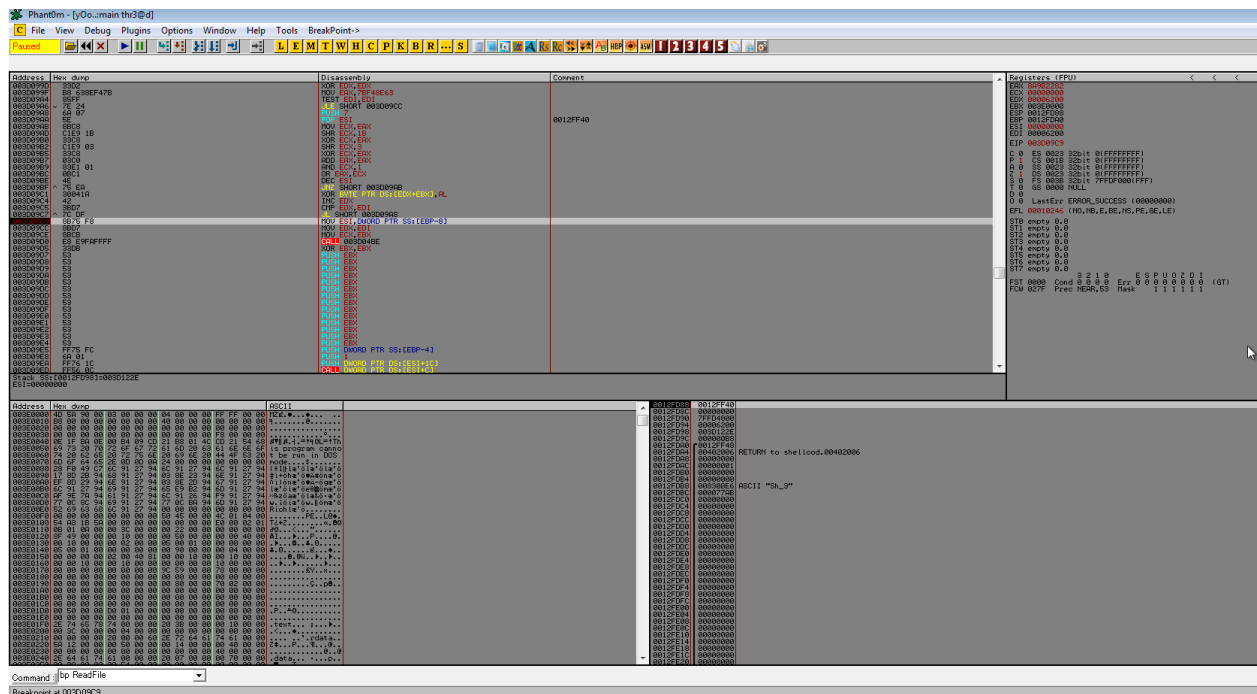


Exhibit 5: Analyst-derived Screenshot of Shellcodeloading 8.t After Custom XOR Cypher

The decoded "8.t" file will have following properties:

File Name: decoded "8.t"

Machine: 0x014C (Intel x86)

MD5: b7499525634a4099d2e19b330e0910d1

SHA1: d53cd84bdd50e27793827d462ea40bd8596417a7

SHA256: 2cfb465858f4264c300d8bb39a7abc542e8da15678f355a994f96bfa5ab54e09c

SSDEEP: 768:26LGcxJ2FbABuHefvV/5R55hwc+CdlRxjF0c0wrH:7j2xG33vf9H

Time Date Stamp: 0x5A1BA854 (11/26/2017 9:53:24 PM)

Size (bytes): 25,088

The decoded malware stores its configuration setting using aPlib compression algorithm. Exhibit 6 shows the pseudo code of WinMain subroutine

80b931ab1798d7d8a8d63411861cee07e31bb9a68f595f579e11d3817cfc4aca

3eb6f85ac046a96204096ab65bbd3e7e
b85368d79231edf57b8f840c876b539657f2d3ae
146aa9a0ec013aa5bdba9ea9d29f59d48d43bc17c6a20b74bb8c521dbb5bc6f4

ab662cee6419327de86897029a619aeb
bf8a297b4a1fd8ee1666be74afca80a8addb145d
6f6ee01e9dc2d8c4c260ef4131fe88dc152e53ee8afd3e66e92d4e1bf5fd2e92

35f456afbe67951b3312f3b35d84ff0a
05e5632ca8c205457d537a6206314e17aad9c9e5
ced7ca9625543d3d3d09f70223cc19f0d99e21792854452df5ba84b3a59d17b8

bd9e4c82bf12c4e7a58221fc52fed705
aa6a121f98330df2edee6c4391df21ff43a33604
7ba05abdf8f0323aa30c3d52e22df951eb5b67a2620014336eab7907b0a5cedf

f8858db5b412deb29800458201912b37
942ef4e9d0ac0cbb356df9cf17fca19220fbed7b
c92a26c42c5fe40bd343ee94f5022e05647876daa9b9d76a4eeb8a89b7f7103d

aca7037286b64b0da05c9708d647c013
d84eb5b6c506d22eaf6bcb2b4f743101d010e721
c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9

e1512a0bf924c5a2b258ec24e593645a
5e39ea9a92662270f616860546277eaa3703ca8a
c7fa6f27ec4f4142ae591f2dd7c63d046431945f03c87dbed88d79f55180a46d

e3867f6e964a29134c9ea2b63713f786
d058567274b5d10f78eebefde62e35f6a389272f
cdf6e2e928a89cbb857e688055a25e37a8d8b8b90530bd52c8548fb544f66f1f

6e843ef4856336fe3ef4ed27a4c792b1
1875db18a7c01ec011b1fe2394dfc49ed8a53956
5860ddc428ffa900258207e9c385f843a3472f2fbf252d2f6357d458646cf362

Domains:

- [eujinonline.sytes\[.\]net](#)
- [api.wsmcoff\[.\]com](#)
- [kc.wsmcoff\[.\]com](#)
- [wsmcoff\[.\]com](#)
- [chemscalere\[.\]com](#)
- [webmail.chemscalere\[.\]com](#)
- [update.chemscalere\[.\]com](#)
- [autoconfig.chemscalere\[.\]com](#)
- [news.chemscalere\[.\]com](#)
- [db.chemscalere\[.\]com](#)
- [autodiscover.chemscalere\[.\]com](#)
- [mail.scsnewstoday.com](#)
- [update.wsmcoff\[.\]com](#)
- [info.wsmcoff\[.\]com](#)
- [store.wsmcoff\[.\]com](#)
- [thyssenkrupp-marinesystems\[.\]org](#)
- [www.chemscalere\[.\]com](#)
- [mail.chemscalere\[.\]com](#)
- [cpanel.chemscalere\[.\]com](#)
- [about.chemscalere\[.\]com](#)
- [ftp.chemscalere\[.\]com](#)
- [catalog.chemscalere\[.\]com](#)
- [scsnewstoday.com](#)

URLs:

- `hxxp://www.thyssenkrupp-marinesystems[.]org/templater.doc`
- `hxxp://www.thyssenkrupp-marinesystems[.]org/templater.hta`
- `wsdl=ftp://185.106.120[.]206/pub/readme.txt`
- `wsdl=fxp://185.106.120[.]206/pub/readme.txt`

IPs:

- 103.243.175[.]181
- 185.106.120[.]206
- 89.245.139[.]187

4. CONCLUSION

At this time, iDefense is still analyzing the data sets collected by proprietary sensors and intelligence operations in order to bolster the findings included in this report. However, there have been no identified reasons to believe that this data set is incorrect.

As indicated by the 2018 Office of the Director of National Intelligence (ODNI) Worldwide Threat Assessment report, China will continue to target cleared defense contractors, IT and communications firms using its robust cyber espionage capabilities.⁸ Moreover, based upon China's integrated and long-term military modernization plans, it could be assumed that Chinese-sponsored collection against maritime technologies that afford advantages to Western and allied naval forces will continue into the foreseeable future.

iDefense believes that DoD supply chain assets, with an emphasis on medium and small contractors, academic institutions and think tanks will continue to be prime targets for adversaries such as MUDCARP. Until requirements, such as those specified in NIST SP 800-171 and "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War", are implemented by members of the DoD supply chain and routinely audited and enforced by the United States government, foreign threat actors will continue to actively exploit these shortcomings.

⁸ "Worldwide Threat Assessment of the Intelligence Community." February 13, 2018.
<https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>

LEGAL NOTICE & DISCLAIMER: © 2019 Accenture. All rights reserved. Accenture, the Accenture logo, iDefense and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from iDefense. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN "AS-IS" BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS ALERT.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 495,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us [@AccentureSecure](https://twitter.com/AccentureSecure) on Twitter or visit us at www.accenture.com/security.