August 2022



INCIDENT INTEL REPORTS

Novel Backdoor Discovered

Deepwatch ATI detects and responds to never before discovered backdoor deployed using Confluence vulnerability for suspected Espionage



Deepwatch's Adversary Tactics and Intelligence group (ATI) recently responded to an incident after a suspicious tool, <u>nb.exe</u> (NBTscan, a tool that scans for open NETBIOS nameservers to find open shares), was observed and escalated to the victim, an organization in the research and technical services sector, by Deepwatch Squad analysts.

> **Note:** To track threat activity clusters observed during incident response engagements, The Deepwatch Threat Intel Team uses Threat Activity Cluster designations (TAC-###) to track similar activity across multiple engagements. The Deepwatch Threat Intel Team tracks the activity covered in this report as TAC-040.

ATI's thorough analysis determined that the attack occurred during the end of May over a seven day period. TAC-040 highly likely exploited a vulnerability in an Atlassian Confluence server. The evidence indicates that the threat actor executed malicious commands with a parent process of tomcat9.exe in Atlassian's Confluence directory.

After the initial compromise, the threat actor ran various commands to enumerate the local system, network, and Active Directory environment. Additionally, the threat actors used RAR and 7zip to archive files and folders from multiple directories, including registry hives. Network logs suggest TAC-040 exfiltrated around 700MBs of archived data before the victim took the server offline.

Furthermore, they dropped a never-beforeseen backdoor, dubbed "Ljl Backdoor", onto the compromised server. You can read Deepwatch's complete analysis with associated observables of this file in <u>Part 2</u> of this threat report.

During ATI's investigation of this incident, an XMRig crypto-miner was observed in the forensic artifacts. Deepwatch assesses that the XMRig related artifacts could be the result of multiple threat actors based on known threat actor activity related to cryptominers. Deepwatch's technical analysis of this loader with associated observables can be read in <u>Part 3</u> of this threat report.

EXECUTIVE Summary

KEY FINDINGS

CVE-2022-26134 was highly likely exploited to gain initial access.

TAC-040 cloned numerous tools from GitHub; one tool, CrackMapExec, serves as an attack framework that contains multiple tools.

TAC-040 has the capability to create or access custom, never-before-seen malware.

It is likely that TAC-040's goal was espionagerelated. However, we can not completely rule out that they were financially motivated.

Organizations that conduct research in healthcare, education, international development, and environmental and agriculture, as well as provide technical services are likely targets of this threat actor.

Note About Estimative Language: To convey the possibility or probability of our hypothesis, the Deepwatch Threat Intel Team employs probabilistic language in our assessments. Because analytical assessments are not certain, we use terms to denote that our hypothesis has a lower or greater than even chance of possibility or probability.

For instance, terms like unlikely, improbable, highly likely, or highly improbable denote that our hypothesis has a lower than even chance of possibility or probability. Likewise, words like likely, probable, highly likely, or highly probable indicate that our hypothesis has a higher than even chance of possibility or probability.

Moreover, a "roughly even chance" denotes that our hypothesis has a roughly 50% possibility or likelihood of occurring. In addition, terms such as "might," "could," or "may" reflect situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented.

Note About Analytic Assurance: Weighing the following factors allows us to assign our assessments and estimates with high, moderate, or low levels of assurance: the complexity of the analytical task; the robustness, number, and applicability of analytic techniques employed, and the degree to which the results coincide; overall source reliability; the degree of corroboration and agreement amongst sources if multiple sources were available; analyst collaboration, expertise, and experience on the subject matter or topic; and finally, we account for any time pressures and deadlines faced by the analyst.

Table of Contents

Novel Backdoor Discovered

Deepwatch ATI detects and responds to never before discovered backdoor deployed using Confluence vulnerability for suspected Espionage

Who is TAC-040?
Attack Analysis6-10
 Exploitation of Confluence Searching for and Collecting Sensitive Data Maintaining Access Novel Backdoor Additional Tools Exfiltrating Sensitive Data
What You Need to Do11
Intelligence Gaps11
Conclusion
Observables13

Who is TAC-040?

To track threat activity clusters observed during incident response engagements, The Deepwatch Threat Intel Team uses TAC-### designations to track activity across multiple incidents. This activity includes all the tactics, techniques, and procedures (TTPs) used; infrastructure; tools and malware employed; and sector and geographic targeting. Tracking threat activity clusters enable the Threat Intel Team to link observed activity across separate incidents..

TAC-040, so far, has targeted a nonprofit organization that conducts research and provides technical services in the following areas: healthcare, education, international development, and environmental and agricultural services.

Analyst Note

Although the Threat Intel Team cannot be certain of TAC-040's intentions and goals, By employing the Structured Analytic Technique of Alternative Competing Hypothesis, Deepwatch Threat intelligence analysts assess that TAC-040 motivation is likely to be espionage-related. However, we cannot completely rule out that the threat actors may be financially motivated.

Additionally, this assessment is supported by the targeting of a non-profit research organization, data staging of specific directories and files, deployment of a custom never before seen backdoor, a webshell deployment utilizing another web server technology on the same system, and the lack of lateral movement to another system for several days, suggesting they were conducting thorough reconnaissance.

Due to the threat actor(s) motivation likely being espionage-related, it is likely to target organizations that

conduct research in healthcare, education, international development, environmental protection, and agriculture or that offer technical services in these fields. However, the threat actor(s) could also target organizations in other industries that operate in these fields.

The Deepwatch Threat Intel Team has developed an "Indicators or Signpost of Change" matrix to monitor any activity linked to TAC-040 that is related to intended targets and their intentions. When new developments arise, we will update our customers accordingly.

TAC-040 has demonstrated the capability to create or access a never-before-seen backdoor, but they also employ numerous open-source tools cloned from GitHub. Additionally, they used a Linode server to store exfiltrated data, which is interesting as we have not seen any opensource reporting of threat actors using Linode to store exfiltrated data.

The victim denied the threat actor the ability to laterally move within the environment by taking the server offline, potentially preventing the exfiltration of additional sensitive data and restricting the threat actor(s) ability to conduct further malicious activities. However, this limited our visibility which may have provided evidence to support whether the threat actor was motivated by financial gain or political espionage.

At this time, the Deepwatch Threat Intel Team cannot link this activity cluster with any level of assurance to any other activity clusters tracked by third parties.



Figure1: The first observed command executed by TAC-040

Attack Analysis

EXPLOITATION OF CONFLUENCE

Deepwatch suspects that towards the end of May 2022, TAC-040 obtained initial access by exploiting a vulnerability [T1588.006] in an outdated Confluence server [T1190] due to the initial command TAC-040 executed (figure 1) [T1033].

Analyst Note

The vulnerability is highly likely to be <u>CVE-2022-26134</u> based on the parent process and proximity to Atlassian's disclosure of the vulnerability a week later, as well as widespread exploitation of Confluence as reported by numerous third parties.

According to Atlassian's <u>security advisory</u>, the vulnerability affects all versions after 1.3.0 and, if successfully exploited, could allow a threat actor to conduct remote code execution (RCE) on vulnerable devices. However, due to visibility gaps, we cannot confirm this hypothesis, and there is the possibility that <u>CVE-2022-22965</u> could have been exploited instead.

cmd.exe /c "cd /d "C:\Windows\system32\"&whoami"

Figure 2: The first observed command executed by TAC-040

SEARCHING FOR AND COLLECTING SENSITIVE DATA.

Once TAC-040 gained access, they issued several commands to enumerate the current user context, running processes, and high-value group memberships. They collected Active Directory data via CSVDE (figure 2) [T1119] and copied the output to a file named 123.csv. TAC-040 then archived 123.csv as 1.rar (figure 3). Additionally, TAC-040 executed ping sweep commands to enumerate an internal IP CIDR block, viewed the available network share drives, and tested their connectivity to Domain Controllers and hosts with names typically associated with mail and backup servers. Furthermore, TAC-040 employed the open-source tool nbtscan (nb.exe) to scan internal IP addresses for NetBIOS name information.

cmd.exe /c "cd /d "C:\Windows\system32\"&C:\ProgramData\Git\csvde.exe -f C:\ProgramData\Git\123.csv"

Figure 3: Active Directory enumerated and copied to 123.csv

C:\ProgramData\Git\rar.exe a c:\C:\ProgramData\Git\1.rar C:\ProgramData\Git\123.csv

Figure 4: 123.csv archived as 1.rar

Once the threat actors completed discovery, TAC-040 executed commands to archive [T1560.001] the HKLM\SYSTEM, HKLM\ SAM, and HKLM\SECURITY (figure 4) registry hives. At this point, the threat actor listed specific directory contents from the available network shares. Additionally, the threat actor attempted to gain access to service and privileged accounts by brute force via password spraying [T1110.003] but failed at all attempts.

cmd.exe /c "cd /d "C:\logs\t"® save HKLM\SAM SamBkup.hiv"

Figure 5: TAC-040 archiving HKLM\SAM



MAINTAINING ACCESS

After investigating the vulnerability used for initial access in the Confluence web application, the Deepwatch Threat Intelligence and Threat Response teams investigated the file system artifacts such as the Master File Table (MFT) and found no evidence or artifacts suggesting the threat actors wrote a traditional webshell to disk to gain persistent access via Apache's Tomcat instance in the Confluence installation directory.

Analyst Note

The threat actor likely utilized a memory-based webshell or opted to run commands directly through the exploit, as no dropper commands or forensic records of an on-disk webshell were recovered. Several opensource reports detail similar defense/detection avoidance techniques concerning the exploitation of CVE-2022-26134, but technical details on these techniques are sparse.

To achieve persistence (as memory webshells do not persist between service or system restarts and vulnerabilities can be patched), TAC-040 created a service on the compromised server named "VBoxxSDS" [T1543.003] that ran the executable "DrSDKcaller.exe," an executable name related to Trend Micro Maximum Security (figure 5). However, we do not know what this service did or its purpose as we could not recover this file. TAC-040 also created another service named "wscsvcs" that ran "wab.exe" (see Part 2 of this threat report). Finally, TAC-040 dropped a custom webshell (jquery.aspx) in a subdirectory of 'C:\ Web' (served by the IIS instance) and executed a script, smbclient_nthash.py.

Analyst Note

It is likely that this script (smbclient_nthash.py) is a "Pass the Hash" tool commonly used by threat actor(s) to attempt to move laterally once an account's hash is obtained. No arguments were passed to this tool. Therefore, we suspect the threat actor(s) were printing out usage instructions for potential usage later.

sc create "VBoxxSDS" binpath= "C:\logs\DrSDKCaller.exe" type= share start= auto displayname= "VirtualBox system service" depend= Tcpip

Figure 6: VBoxxSDS service creation command

NOVEL BACKDOOR

A backdoor (wab32res.dll), dubbed "ljl Backdoor", was also loaded onto the infected server. The Deepwatch Threat Intel Team has determined this backdoor is a never-before-seen and persistent backdoor [T1587.001].

Ijl Backdoor has the following capabilities:

- ✓ Reverse Proxy.
- Query whether the victim is active or idle.
- Exfiltrate files/directories.
- Load arbitrary and remotely downloaded .NET assemblies as "plugins."
- ✓ Get user accounts.
- Get the foreground window and window text.
- Get victim system information, such as CPU name, GPU name, hardware id, bios manufacturer,
- ✓ Mainboard name, total physical memory, LAN IP address, and mac address.
- Get victim geographic information, such as ASN, ISP, country name, country code, region name, region code, city, postal code, continent name, continent code, latitude, longitude, metro code, time zone, and date and time.

Analyst Note

We suspect it is new, as we could not find any internal or open-source reporting on this backdoor. You can read Deepwatch's complete analysis with associated observables of this file in <u>Part 2</u> of this threat report.

Tag: IP-Connection Version: 1.0.0.3 Loader path: C:\Program Files\Common Files\Securitys\wab.exe C2: 209.58.191.235:443;u7cejx.kf2y3o.com;443; Mutex: 319432a.3d6a-4f8f-a366-4f8f-dd20b083 Server Signature: KnxaQlex5Kzg9AlVf/bn0Y01xnEbs1Gp1K0PezyDXMiachh5GNLjbukBchyIjU7xpaHPCC3806yPtrbDc5tZunGKM1JJ+mb1KWu07H u/nv+q8UjvnKxOMgAn+bEROVo-w154guP4Rpw23CNxsG6az7oU/g19TN3r/rkOBC/c5QkXh1BzGmEYjFcik7GAwHrpxw7jgq5u9iN3uLDTy1kNjzM81/A IL9a/+xrY77/Wte611M0Brw5vKuG6su52d/eEjgvtjvuXjVbciE9OsGx31mu4pKCXUFj7uJna7j00Vxbegbg8iFlyOphmFzULKC1HXMEVhxcm/c66033ugvN /aTorAOD9WOXdzp2bywWxb65kgJBdWenL3-egubUQITVhoqkxZZTgCPT8CeDA0mIKCTW157uJna7j00Vxbegbg8iFlyOphmFzULKC1HXMEVhxcm/c66033ugvN /aTorAOD9WOXdzp2bywWxb65kgJBdWenL3-egubUQITVhoqkxZZTgCPT8CeDA0mIKCTW157uJa7j00Vxbegbg8iFlyOphmFzULKC1HXMEVhxcm/c66033ugvN /aTorAOD9WOXdzp2byWxb65kgJBdWenL3-egubUQITVhoqkxZZTgCPT8CeDA0mIKCTW57kUJQ2DDA1samwgU2VgVMVzdENBKD21JBT785NYj0K15ire58WvW7UVQ3QDNVRcaTZ0ygQ2fDvAcFi987TcWPxEnje44c1Y= MIEFjCCAtagavIBAg1QAM1e25bMPPv172Ke89V0ATNBkgdqkhiG9W0BAQ0FADA7MRYWFAFV0VQQDDA1samwgU2VgVMVyIENBMLCAXDTIyMDIyNTAOMTQ1MFoY DzkSOTkxMjMxMjM10TUSWjVMRWr4xAVDVQQDDA1samwgU2VydmVyIENBMLTIjANBgdqhkiG9W0BAQEFAA0CAQ8AMIICCgKCAgEAvcEYJf8/DEAW9CtKu4NL Avb/zoZp60AxREzfo38Wv+//SURdWfidhp6jn3quucWJNd8iKbcEbDQ6QdTNMmarXX63Kk-7/cS1UHLEUXxENg705bBTB0ZLEaXf1d1mmC5jj2D/L 0hrFmE9mkszrHrufQyg7gKi9mW/5/OHT54X+g2PRJapzCRcnsa2rpq4c2PHFYKQ/oqM6wxmVFGdjCa2sAImCGrn87ReaM3f1SHEhE41vg7XxuMW826hR-65 NuwypvfS30eI/D0LogT4CQdbpHYKae/igQLDS8mhxUgBdwSf5r7tKa31+RKLcD1Bwd0p61ZBwceRVP19T/oBL302Vo3yM1yOEuT0W2J3S029dXWPZSy2V 1JycEK5+x7F9jAbC02025SPHSwFvCsdEnjPFFKOW+mi16cJ5Hk2n5/UUMB2ANDF97Ztd1gsGU1LCAM7zut000PJNgaTk2VxgVUJ02S02JdXmW2S9dXWPZ3J22VZMBVP7/Ztd1gsGU1LCAM2xUB0950UZ5VxJ1yD&2J3022VZMB29202VZMBPF7Ztd1gsGU1LCAM2xUB0950202V3VJNBV491BW2590Z2V2XVBW RnwypvfS30eI/D0LogT4CQdbpHYKae/igQLDS8mhxUgBdwSf5r7tKa31+RKLcD1Bwd0P6J2BwceRVP19T/oBU2O2V3JM1yOEuT0M2J3S029dXNPZ332 KnwypvfS30eI/D0LogT4CQdbpHYKae/igQUDS8MhXBdBdwSf5r7tKa31+RKLcD1BwdW96D3Dv4Vg1DV0B0BVEFLN15xNAbbcVQLt6Anf1VULteCMAM86 AludewEEAvgF	
Loader path: C: Program Files\Common Files\Securitys\wab.exe C2: 209.58.191.235:443;u7oejx.kf2y3o.com:443; Mutex: 3149432a-3d6a-4f8f-a5d6-4f64d20b083 Server Signature: KnxaQIex5Kzg9Alvf/bn0Y01xnEbsIcp1k0PezyDXMiach5GNLjbukBchyIjU7xpaHPCC3806yPtrbDc5tzunGKMIJJ+mb1KWu07H uVnV+q8UiynKxOMqNA+bEROV0-w154guP4Rpwz3CNxei6+RZrOU/g19TN3r/rk0E2/c50kXhJBzGmEYjFcik7GAwHrpxWJgqQsU9iN3uLDTylkNjzM81/A Ll9a/+xrV77/Wtc6JIMQBrwSVKuG6suS2d/eEjgYtjvuXjVbCiE90sGx3iHru4pKCXUfj7uJna7j00VNbegbg8iFJV0phmFzULKC1HXMEVhxCm/G6033ugvN /aTorA0p9w0XdzpzbywWxb63KgJWemkJ+egwbU0TTvhoqkxZZTgCPT8GeDAOmIKcTEX5Xt0/fzWjGrUef1f7ostutxzwdiBgkbqQa1+02axZH/q1AaAlHJRh cYPK0PZ/+LvMBzqhkoIYdLRhIv9eibpnC5ckUCX+uwTXTTUCRXs+opsgrsJ2Sx5Y6ykdL2IL+57ELQIMWfsS0X5g7Db2oGHVGsFvSddVZkvEqjVP1s/xUta cG4ufjZtLllocqcZIW6ej8irtLnEjhr08Vp13BT/83NYj0klsire58wYwfvup3gINuVRcatZ0yg02fDvAcFi9B7TcWPxEnje44C1Y= MIE7jCCAtagAwIBAgIQAM1ez5bMPPvTZ/ke8pv0ATANBgkqhkiG9w0BAQ0FAAD4MRYwFAYDVQQDDA1samwgU2VydmVyIENBMCAXDTIyMDIYNTA0MTQ1MFOY Dzk5oTkxMjMxMjMIOTUSWjAVMRYwFAYDVQQDDDA1samwgU2VydmVyIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvcEYJF8/DEAW9CtKu4NL Xvb/zoZpE0AxREzfosa9w+//SURdWfidhp6jn1quucwbJNdBikDxEcbD0Q6dINwnarXX63KK+7/7cS1UMLHEUxxEhgr705bBrIBQ7LEaXfJd1mmC5jJ2D/L 0hrFwE9mkszrHruf0yg7gKi9nw/5/DrTS4X+g2PRJapzCRcnsa2rpq40c2PHfYK0/oqM6wmVPGdjCa2sAImCGr87ReaM3f1SHEhE4iVq7XKUMWB26hR+65 w1HKApY2AhUyutS7cs8fEiNZ0YRnvj9QbMS92dzYLWJBP77zIJjsGU1UCAW7Auf00N/Wym2VENB06PUJTsfuS9u+SC86dqHSmvpD94Yw/UCTuz1juw KnwypyfS30eI/O0LogT4CqdbpHYKae/iqz0LDS8mhxUgBdwsf5r7/Kq31+RkLcCJiBwM0p61ZBwceRVP19T/0BU2OZvoJyM1y0EuT0M2J3So29dXNP2J3A2g 4JUdewEB/wQFMAMBAf8wDQYJKoZThvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL0T/9zuW63JJ1mFrh7nJJ9xVtif6087gL eax3wcg0DD6jvsUUh2+S2E7cg1yAW1ZdDLe0gZ/TNh6kb41Fuj5LXkFokBkoXyjuL+w0LIANYAzkyInjaE10MKRW2wBU8grgmjyEv111dbu4Sk8gw3T 783du9a10hvZ0W023bFL20L003H+z0L023/xz2jms6c/0Hz2D9vnzj0xoR8VAB8J2FESbM0P072WL89F0x50HJ3jHyAC+2HN9gXVeif6087gL eax3wcg0DD6jvsUUh2+S2E7cg1yAW1ZdDLe0gZ/TNh6kb41Fuj5LXkFokBkoXyjuL+w0LIANYAzkyInjaE10MKRW2WBU8grgmjyEv111dbu4Sk8gw	
<pre>C2: 209.58.191.235:443;u7oejx.kf2y3o.com:443; Mutex: 3149432a-3d6a-4f8f-a566-64f64d20b083 Server Signature: KnxaQIex5Kzg9AlVf/bn0Y01xnEbs1Gp1kQPezyDXMiachf5GNLjbukBchyIjU7xpaHPCC3806yPtrbDc5tZunGKM1JJ+mb1KWu07H uVnV-q8UiynKx0MqNA+bER0V0+w154guP4Rpwz3CNxei6+RZrou//g19TN3r/rk0B2/c5QkXhJBzGmEYjFcik7GAwHrpxwJgqQsU9iN3uLDTy1kNjzM8I/A II.9a/+xrY77/Wte51JMQBFWSVKuG6suS2d/eEjytjvuzjYbCiE09oSkX3iHru4pKcXUfj7uJna7j00Vhbegbg8iF1Vg0hmEzULKC1HXMEVhxCm/G6033ugvA /aTorAOp9wOXdzpzbywWxb63KgJWemkJ+egwbUQITvhoqkxZZTgCPT8GeDAOmIKcTEX5Xt0/fzWjGrUef1f7ostutxzwdiBgkbqQa1+02aNZH/q1AaA1HJRh cYPKOPZ/+LvMBzqhkoIYdLRhIv9eibpnC5ckUCX+uwIXTTUCRXs+opsgr5J25x5Y6ykdL2IL+57ELQIMWfs5OX5g7Db2oGHVGsFv5ddvZkvEq0jVP1s/xUta cG4ufjZtlllocqcZTW6ej8irtLnEjhr08Vp13BT/83NYj0k1sire58wWrvup3g1NuVRcaT20ygQ2fDvAcFi987TcWPxEnje44C1Y= MIIE7jCCAtagAwIBAgIQAM1eZ5bMPPvTZ/ke8pv0ATANBgkqhkiG9w0BAQ0FADAVMRYwFAYDVQQDDA1samwgU2VydmvyIENBMCAXDTIyMDIyNIA0MTQ1MFov Dzk5OTkxMjMxMjMIOTUSWjAYMRYwFAYDVQDDDA1samwgU2VydmVyIENBMILC1jANBgkqhkiG9w0BAQEFAAOcAg8AMITCgKCAgEAvCEY1F8/DEAW9CtKu4NL Xvb/zo2pE0AxREf5osa9w+//SURdWfidNp6jn1quucwBJMdBixbEcEbDQGQIINMmarXX63KK+7/7cS1UMLHEUxxEhgr705bBFIBQ/LEAXfJd1mmC5jJ2D/ UhFWE9mkszrHrufOyg7gki9nw/5/DrTS4X+g2PRJapzCRcnsa2pq4Qc2PHfYKQ/oqM6wmWPGdjca2sAImCGr87ReaM3f15HEhte1ivg7XkuMWB26hR+65 w1HKApY2AhUyutSTzrGx9FCs8iF1M2I0YRnvj9QkMS9Z0t2wIMbP7ZIdjsGU1UCAmYzut00n/Wyym2txqjIY1SvWN1Wv491uBzo590UZ5vrxJjDwkJV2yKV IJycEK5+x7f9jAbCQoZvSSPHSwfVc5dEnjrPFKOw+mildEJSH2R7zIgsGU1UCAmYzut00n/Wyym2txqjIY1SvWN1Wv491uBzo590UZ5vrxJjDwkJV2yKV KwypyfS30eI/D0Loq74CQdbpHYKae/iqzQLDS8mhxUgBdwsf5r7tKq3t+RkLcCJiBwWDp61ZBwceRVP19T/0BUZOZv0JyM1yOEuT0M2J33co294NP23A2g V/b2a6n/y1S739E1/SNW0WU/XBABBysE25SeMaaDUP3p15FDxxiSHkh1adzJECAwEAAAMMMDAWHQVDN00BBYEFN/SISu6BcVQLt66hf1vULtecMaMA8g A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL0T/9ZuW63JJirMFrh7nJ349xVtif60B7gL eax3wcg0DD6jvSUUh2+52E7CgT5x4MW1ZRdDLe0gZ/TNh6kb41Fuj5LxKFoKBkAxyjuL+w0LTANYA2ky1njaE10MKRW2WBU8grmjyeV1JIdbu4SkEgwsT 783du9a10hvZ0WE3pF9167cJvybmyZv5ztIJmkBk041Fuj5LxKFoKB</pre>	
Mutex: 3149432a-3d6a-4f8f-a566-64f64d20b083 Server Signature: KnxaQlexSkzg0Alvf/bN0V0lxhEbslGplkQPezyDXMiachh5GNLjbukBchyIjU7xpaHPCC3806yPtrbDc5tzunGKMlJJ+mblKWu07H uVnV+q8UiynKxOMqNA+bER0V0+wl54guP4Rpwz3CNxei6+RZrOu//g19TN3r/rk0B2/c5QkXhJBzGmEYjFcik7GAWHrpxwVJgqQsU9iN3uLDTylkNjzM81/A IL9a/±xrY77/wtc6J1MQBrWSVKuG6suS2d/eEjgYtjvuXjVbCiE090sKX3iHru4pkCXUfj7u1na7j00VNbegbg8iFJyOphmEzULKC1HXMEVhxCm/G6033ugvN /ATorAOp9WOXdzp2bywWxb63KgJWemkJ+egwbU0ITVhogkxZZTgCPT8GeDAOmIKCTEX5XtO/f2WjGrUeT1f7oStutzxzwdiBgKbqQal+02NRH/aAA1HJRh cYPK0P2/+LVMBzqhkoIYdLRhIv9eibpnC5ckUCX+uvTXTTUCRX=opsgrSJ2Sx5V6ykdL21L+57ELQ1MWfsS0X5g70b2oGHVGSFvSddvZkvEqQjVP1s/xUta CG4ufjZR11locqcZIW6ej8irtLnEjhr08Vp13BT/83NYj0k1sire58WYWrup3gINuVRcaTZ0ygQ2fDvAcFi9B7TcWPxEnje44C1Y= MIIE7jCCAtagAwIBAgIQAM1eZ5bMPPvTZ/ke8pV0ATANBgkqhkiG9W0BAQ0FADAVMRYWFAYDVQQDDA1samwgU2VydmVyIENBMCAXDIJyMDIyNTA0MTQ1MFoY Dzk50TkxMjMxMjM10TU5WjAYMRVFAYDVQDDA1samwgU2VydmVyIENBMIICIjANBgkqhkiG9W0BAQEFAAOcAg8AMIICCgKCAgEAvCEYJFB7DEAW9CtKu4NL Xvb/zo2FE0AxREf5ca3gW4//5URdWfidNp6jinjquucWbJM8biKbxEcbD6QdJINMmarXx63KK+7/7cS1UMLHEUxsKBgr705bBFIBQ/LEAXfJd1mmCSjJ2D/ 0hrFwE9mkszrHruf0yg7gKi9nW/5/DrT54X+g2PRJapzCRcnsa2rpg4Qc2PHFYKQ/oqM6wxmVPGdjca2sAImCGrn87ReaM3f1SHEhE4ivg7XkuMWB26hR+65 w1HKApY2AhUyutSTzrGx9Fcs81FIMZT0YRnyJ9QkMS9Z0t2MIMBP/7zIdjsGU1UCAmYzut00n/Wyym2txqjIY1sVNNIW491UBzo590UZ5vrxjjDwk3V2yKV IJycEK5X76j3AbcQozVsSPHSwFvCs6BnjPFFK0W+mi16GJSH2R7KGJB2CHUPB3dL/C5JBWWp6J2BwceRVP19T/0BU20Zv0JyM1yOEUT0M2J3S029dXNPZ3sA2g V/b2aGn/y1S739c15xWQwu/vXBABByseZESseMaaDUP3p151FDxxi5Hkh1adzJECAwEAAMMyMDAWHQDVR00BYEFN/1SXNGbbcVQLt6Snf1vULtecMaMA8G AlUdEwEB/wQFMAMBAf8wDQYJKoZIHNEAADJ9J51KFKcb41FmL890yVdaUfWDgd8Noi0gHLGPTR9VztEFbLoT/9ZuW67J1JrMrrh7nJ194yxt11f60B7gL eax3Wcg0DD6jvSuUb2+S2E7CgT5x4WW12RdDLegZ/TNh6kb41Fuj5LXkFokBkoXyjuL+w0LTANXA2ky1njaE10MKRW2W8U80gmjmyEV111dbu4SkEgws1T r83du9a10hvZ6WE3pF9167_07ypnXz/Sv2UML8FL95BNQK0FnHDZ2D9nzCE5Dg9v2tEJBJv0K0CM2Yrk2Mytd6Ywn9QTGwGGpIrooSLRrqr77 Z3+rCoy4vwpw+1eHrWZdkZ8ByP01G20JSWL2Fj058HX04L6Fj058PNQVCF1PDZ9nzCE5Dg9v2te5Dg9v2te7k2Mytd6Ywn9QTGwGGFJIroS	Loader path: C:\Program Files\Common Files\Common Files\Securitys\wab.exe
Server Signature: KnxaQIex5Kzg9Alvf/bn0Y0lxnEbs1GplKQPezyDXMiachh5GNLjbukBchyIjU7xpaHPCc3806PtrbDc5tzunGKM1JJ+mblKWU07H uVnV+q8UiynKxOMqNA+bER0V0+wl54guP4Rpwz3CNxei6+RZrOu//g19TN3r/rk0B2/c5QkXhJBzGmEYjFCik7GAwHrpxwVJgqQsU9iN3uLDTylkNjzM81/A IL9a/+xrY77/tte6J1MQBrwSVKuG6sUS2d/eEjgYtjvuXjVbCiE90sGx3iHru4pKCXUFj7Una7j00VNbegbg8iFJPOphmFzULKC1HXMEVhxCm/G603ugvN /aTorA0p9w0XdzpzbyWkb63KgJWemkJ+egwbUQITvhoqkxZZTqCPT8GeDAOmIKCTEX5Xt0/fzWjGrUef1f70stutxzwdiBgKbqQa1+02aNZH/q1AaAlHJRh cYPK0PZ/+LvMBzqhkoIYdLRhIv9eibpnC5ckUCX+uwTXTTUCRXs+opsgrSJ2SX5Y6ykdL21L+57ELQIMwFs50X5g7Db2oGHVGSFvSddVZkvEqjVP1s/xUta cG4ufjZtL1LoqcZIW6ej8irtLnEjhr08Vp13BT/83NYj0klsire58WVWfvup3gINuVRcaTZ0yg02fDvAcFi9B7TCWPxEnje44C1Y= MIIE7jCCAtagAwIBAgIQAM1eZ5DMPPvTZ/ke8pv0ATANBgkqhki69W0BAQ0FADAMRYwFAYDVQQDDA1samwgU2VydmVyIENBMCAXDTIyMDIyNTA0MTQ1MFoY Dzk5oTkxMjMxMjMIDTU5WjAYMRYwFAYDVQQDDA1samwgU2VydmVyIENBMLC1jANBgkqhki69W0BAQEFAAOCAg8AMIICCgKCAgEAvCE7J7B7DEAW9CtKu4NL Vxb/z0ZpE0AxREzf0sa9wV+//SURdWFidPp6jn1quucWbJNdBiKbxEcbDQ6QdINWnarXX63KK+7/7cS1UMLHEUxxEhgr705bBrIBQ7LEaXfJdImmC5jJ2D/L 0hrFwE9mkszrHruf0yg7gKi9nw/5/DrT54X+gZPRJapzCRcnsa2rpq4qc2PHfYKQ/oqM6wmWPGdjCa2SAImCGr87ReaM3f1SHEhE4ivg7XkuMW826hR-65 W1HKAPY2AhUyutSzr6x9FcS8iF1MZ10YRnvj9QkMS92OtZWIMDP7/ZIGjsGU1UCAmYzut00N/Wym2tBNBUCV00B9VEFN/15X0BL20590U25vrxJjDw&Jv2VkV 11ycEK5+X7f9jAbCQoZvS5PHSwfVcSdEnjrPFK0ww+mi16cJ5Hk2n5/UymibZINoLP8jdL/L65S0qHyF0DsDF9JTsfuS9u+SCB6qHSmvpD94Yw7UCTu21juw KnwpyfS30eI/00LogT4CqdbpHYKae/iq2QLDS8mhxUgBdwsf5r7tKq3t+RRLcC1iBwW0p6JZBwceRVP19T/0BU2OZvoJyM1yOEUT0M2J3S029dXNPZ3sA2g V/b2a6n(y1S739C15xW0Wu/VXBABByS2ES5seMaaDUP3p15IDFxxi5Hkh1adzJECAwEAAAMMVAM4WQV0N00B8VEFN/15XNB0bcVQLt6Knf1vULteCMaMA8G A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL0T/9ZuW673JJimFrh7nJ349xvtif6087gL eax3wcg0DD6jv0sUUh2+S2E7Cg7VyNX2V5VUJ880HEC3aFthFkLadZJECAwEAAAMMVAMWAWV0N00B8VEFN/15XM4VB40BgrgmjyEV11Idb4SkBgws1T z83du9a010hvZ0WD23bF25Z75v4MW1ZRd0Le0gZ/TNh6kb41Fuj5LxKF6kBkoXyjuL+w0LIANVA2ky1njaE10MkRW2WBU8grgmjyEV11Idb4SkBgws1T z83du9a10hvZ0WD425Hz2L0J374X	C2: 209.38.191.235:443;U/06]X.KT2/30.C0m:443;
uvnv+q8UijmkxoMqNA+bEROV0+w15ÅguP4Rpwz3CNxei6+RZrou/jgl9TN3r/rkOBZ/c5&kXhJBzčmEvjFcik7GAwHrpxwJgqQsU9iN3uLDTylkNjzMSL/A IL9a/+xrY77/wte6J1MQBrwSvKuG6suS2d/eEjgvtjvuXjYbCiE90sGX3iHru4pKCXUFj7uJna7j00VNbegbg8iFlyOphmFzULKC1HXMEVhXcm/G6O3ugvN /aTorAOD9WOXdzpzbywWxb63KgJWemkJ+egwbUQITvhoqkxZZTgCPT8GeDAOmIKCTEX5XtO/fzWjGrUef1f7oStutxzwdiBgkbqQal+02aNZH/aAAlHJRh cYPKOPZ/+LvMBzqhkoIYdLRhIv9eibpnC5ckUCX+uwTXTTUCRXs+opsgrSJ2Sx5Y6ykdL2L1+57ELQIMWfsSOX5g7Db2oGHVGsFvSddvZkvEqQjVPls/xUta cG4ufjZrtllocqcZIW6ej8irtLnEjhro8vp13BT/83NYj0klsire58wiYntuP3gTuVRcaTzQJ0gQ2fDvAcFi9B7TcWPxEnje44C1×= MIIE7jCCAtagAwIBAgIQAM1eZ5bMPPvTZ/ke8pV0ATANBgkqhkiG9W0BAQ0FADAYMRYwFAYDVQQDDAlsamwgU2VydmvyIENBMCAXDTIyMDIyNTA0MTQ1MFoY Dzk5OTkxMjMxMjMIOTU5WjAYMRVwFAYDVQQDDALsamwgU2VydmVyIENBMIICIjANBgkqhkiG9W0BAQEFAAOCAg8AMIICCgKCAgEAvCEY1F87DEAW9CtKu4NL Xvb/zo2pE0AxREf5osagW+//SURdWfidNp6jnjaucwBJNdBiKbEcbD06QdINWnarXX63KK+7/7cS1UMLHEUxxEhgr705bBFIBQ7LEAXfJd1mmC5jJ2D/L 0hrFwE9mkszrHruf0yg7gKi9nw/5/DrTS4X+gZPRJapzCRcnsa2pq4Qc2PHfYKQ/oqM6wxmVPGdjca2SAImCGrn87ReaM3f1SHEhE4ivg7XvxMJWB26hR+65 w1HKApY2AhUyutSTzrGx9FCs8iF1M2I0YRnvj9QkMS9Zot2WIMbP7/zIdjsGU1UCAmYzut00n/Wyym2txqjIYlsVWN1Wv491UBz050UZ5vvxJjDwkJV2yKV IJycEK5+X7F9jAbCQoZvSSPHSwfVcSdenjrPFKØwv+mil6CjSHk2ns/Uym1bZINOLP8jdL/c65S0qHyF0DsDF9JTsfuS9H+SCB6qHSmvpD94YWUCTUZ1juw KnwpyvFS30eI/D0LogT4CQdDpHXkae/iqz0LDS8mhxUgBdwsf5r7Kkg3t+RkLc2iBw0p6jZBwceRVP19T/0BU20Zv0JyM1y0EuT0M2J3So29dXPZ2x2g V/b2aGn/y15739E1/sWQUw/XBABByseZ5seMaaDUP3p151FDxxi5Hkh1adzJECA&AAMMDAwHQDVR00B8YEFN/1sXMBbevQ1t6Ksfr1vUtteCMaAA86 A1UdEwB/wQFMAMBAf8w0QYJKoZIhvcNAQENBQADggBAChe1fmL890yYddUfWDgd8Noi0gHLGPTR9vztEFbL0T/9zuw6r3JjirMFrh7nJ349xVtif60B7gL eax3wcg0D06jvSuUh2+S2E7CgT5x4MW1ZRdDLe0gZ/TNh6xb41Fuj5LXkFokBkoXyjuL+w0LTANYA2ky1njaE10MkRW2wBU8BgrmjyEV11Idb4SkBgws1T r68d4Uga10hvZ6WL28B3pF167_c07ypnx2v5zt0JaFthatHeftefJ6qU21P2Ij4+AZbEkusyQMw0pnyn21v0ExcMZ2rk2Mytd6YwH34CrNw8Q1F0w5F77 Z3+rCoy4vWwpw+1eHrWZdk2B3B916L034K2FJaFth4EF16J05NRV2F4A	
IL 9a/±xrY77/wte6j1MQBrWsVKuG6süS2d/eEjgYtjvuXjVbCiE005xX3iHru4pKCXUfj7uJna7j00Vxbegbg8iF]yOphmFzÜLkC1HXMEVhxCm/G6033ugvN /aTorAOp9w0XdzpzbywWxb63KgJWemkJ+egwbUQITvhoqkxZZTgCPT8GeDAOmIKCTEXSXt0/fzWjGrUef17oStutzzwdiBgkbqQal+02aNCH/q1AaAlHJRh CYPKOPZ/+LvMBzqhkoIYdLRhIY9eibpnC5ckUCX+uwTXTTUCRXs+opsgr5J2Sx5Y6ykdL2IL+57ELQIWwfs5DX5g7Db2oGHVGsFvSdUZkvEqQjVPls/xUte G4ufjZRt1locqcZIW6ej8irtLnEjhr08Vpl3BT/83NYjOklsire58wYwfvup3gINuVRcaTZ0ygQ2fDvAcFi987CWPxEnje44Cly= MIIE7jCcAtagAuBAgIQAMI25DWD4TANBgkqhkiG9W0BAQDFAAAMRYWFAYDVQQDDAIsamwgU2VydmVyIENBMCAXDTIyMDIyNTAOMTQIMFoY Dzk5OTkxMjMxMjMIOTUSWjAYMRXwFAYDVQDDAIsamwgU2VydmVyLENBMIICIjANBgkqhkiG9W0BAQEFAAOcAg8AMIICCgKCAgEAvCEY1F87DEAW9Ctku4NL Xvb/zoZpE0AxREzf0sa9wV+//SURdWfidNp6jnJquucWbJNdBikbxEcbDQ6QdINWnarXx63Kk+7/7CS1UMLHEUxxEhgr705bBrIBQ7LEaxfJdTmmCSjJ2D/L OhrFwE9mkszrHruf0yg7gKi9nW/5/DrTS4X+gZPRJapZCRcnsa2rpg4Qc2PHfYKQ/oqM6wxmVPGdjCa2sAImCGn87ReaM3fISHEhE4iVg7XkuMW26hH+65 w1HKApY2AhUyutSTzrGx9Fc88iF1MZIOYRnvj9QkMS9Z0t2WIMDP7/ZIdjsGUTUCAmYzut00n/Wyym2txqjIYlsVWNIW491UBzo590UZ5vrxjjDwkJV2VKV IlyccK54X7f9jAbCQoZvSSPHSWFvC5dEnjrPFKOMw+mi16c1SHk2ns/JHk1Ad2JECAwAAMMMDAWHQVDVR00BBYEFN/lsXnSbbcvQLt6Anf1dULtecTMAMA8G AlUdEwEB/wQFMAMBAf8W0PJXoZIHvCNAQENBQADggBBAChe1fmL890yYdaUfW0gd8Noi0gHLGPTR9VZtEFLoT/92UW08YEISNGbbcvQLt6Anf1dULtecTMAMA8G AlUdEwEB/wQFMAMBAf8W0PJXoZIHvCNAQENBQADggBBAChe1fmL890yYdaUfW0gd8Noi0gHLGPTR9VZtEFLoT/92UW6731iFFFn71349xt11dbu4SkBgws1T r83du9a10hvZ6WBAf88by2vC22rJNb6xb1F60BZyngvLcff0g0VF9JTSAMBAf8ABgvc2C2G70Thh6xb41FmL890yYdaUfW0g0FN02SNZHMB2x2kF2Myt01NAaE+kY7/2JHmbz/C07VyBNXF2VS2MW1ZKADLe0gZ/TNh6xb41FmL890yYdaUfW0g0FN02SNZHMVQVZCWDB8YEFN/lsXnGbbcvQLt6Anf1dHu4KBgws1T r83du9a10hvZ6WB478by20X2Lf6ADJAFFFFFF6J6qUC1P2Ij4+AZbEkusyQMW0pnyn2Iv0ExcMZYrk2Mytd6Ywn9QTGwG6pIrooSLRrqr77 Z3+rCoy4vwpw+1eHrwZdE/L93BNQ2K2L0FJ3fbRNAdCrHbZ2D9nzC55D9r2+S1MjzwDh00g3H+z0LG3KJK1Ag2KrWA2KJMyt0A3H+z2CFVB47WL4AZ	Server Sterver Sterver Analytex Xzg9ATVT/000V01ArbbS19D1K0P220XMTAChDSNLJDUKBChyJJU/XDAHPCC38009P1P0DC512UnGKM1JJH7bbLK0U0/H
/ATOrAOp9w0XdzpzbywWxb63KgJWemkJ+egwbUQITVhoqKxZZTQCPT8GeDAOmIkCTEX5Xt0/fzWjGrUef1f7ostutxzwdiBgkbqQal+02aNZH/qlAaAlH7Rh cYPK0PZ/+LyMBzqhkoIYdLRhIV9eibpnC5ckUCX+uwTXTTUCRXs+opsgr5J2sX5Y6ykdL2LL+57ELQIMWfs50X5g7Db2oGHVGsFvSddVZkvEqQjVPls/xUta cG4ufjZRtllocqCZIW6ej8irtLnEjhr08VplBT/83NYj0klsire58wYWfvup3gINuVRcaTZOygQ2fDvAcFi9B7TcWPXEnje44CIY= MIIE7jCCAtagAwIBAgIQAMleZ5DMPPvTZ/ke8pv0ATANBgkqhki69w0BAQ0FADAVMRYwFAYDVQQDDAlsamwgU2VydmVyIENBMCAXDTIyMDIyNTAMUTQIMFoY Dzk5OTkxMjMxMjMIOTU5WjAYMRYwFAYDVQQDDAlsamwgU2VydmVyIENBMLCIjANBgkqhki69w0BAQEFAAOCAg8AMIICCgKCAgEAvCEYJB7DEAW9CtKu4NL Xvb/zoZpE0AxREzfosa9wV+//SURdWfidNp6jnJquucwbJNdBiKbxEcbDQ6QdINMnarXx63KK+7/7cSlUMLHEUXxEhgr705bBrIBQ7LEAXfJdImmC5j2D/L 0hrFwE9mkszrHruf0yg7gki9nw/5/DrT54X+gZPRJapzCRcnsa2rpq4qc2PHfYKQ/oqM6wxmVPGdjCa2sAImCGrn87ReaM3fISHEbE4ivg7XxUMWB26hR+65 wlHKApYZAhUyutSTzr6x9Fc58iF1MZ10YRnvj9QMS92OtZWIMbP7/ZIGjsGU1UCAmYzut00N/Wyym2txqjIYlsVwNIWv49lUBzo590U25vrxJjDwkJV2yKV 1lycEK5+X7f9jAbCQoZVS5PHSwfVc5dEnjrPFK0ww+mi16cJ5Hk2nS/UymibZINoLP8jdL/L65S0QHyF0DsDF9JTsfus9u+5CB6qHSmvpD94YW7UCTu21juw KnwpyfS30eI/O0LogT4CqdbpHYKae/iq20LD58mhxUgBdwsf5r7tKq3t+RKLcCJiBwW0p6lZBwceRVP19T/0BU20Zv0JyMJy0EuT0M233S029dXNP23sA2g AlUdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL0T/92uW6r31JirMFrh7nJ349xVtif60B7gL eax3wcg0DD6jv0sUUh2+52E7CgT5x4WW1ZRdDLe0gZ/TNh6kb41Fuj5LxKFokBkoXyjuL+w0LIANYA2ky1njaE10MkRW2WBU8grgmjyEv11Idb4SkBgws1T z83du9a10hvZ0Mb23FC97Cg7ysQwLdPfjop58HzW8K05PNKCNHDz2D9nQeRZPBVAKWQM0Pmyn21v0ExoCMZVrkMydGfWr9QTGwG9FrooSLRrq77 z3+rCoy4vWwpw+1eHrwZdE/L93nxqz7ySQwLdPfjop58HzW8TX05NK0F0HDZ2D9nQEC5Dgv+s1Mjzwb0PgH1VmgfTLFRh+G+PovTpq9hr72Vtt+n24A	an in the of yn kong net berovot wit Jegur en pwz Schnet of Kztowy gi s in Strike Cycken i bezanie i sec i kroawni pzwy golgso si Nou Liby i kn j zmół / A Ni 9 a / zwyz 7 / wite foi 1100 R misy Win Genz a dry tany i wite i of cigo go z si mala netwy wite i bana i ma
cvPGP2/+LvMBzqhkoIydLRhIv9eibpnC5ckUCX+uwTXTTUCRX5+opsgr5J2Sx5Y6ykdL2L1L+57ELQIMWfs50X5g7Db2oGHVGsFv5ddV2kvEqQjVPls/xUta CG4ufj2RtllocqcZIW6ej8irtLnEjhr08Vpl3BT/83NYj0klsire58wYwfvup3gINuVRcaTZ0yg02fDvAcFi9B7TcWPxEnje44ClY= MIIE^jCcAtagAwIBAgIQANle25bMPPvTZ/ke8pV0ATANBgkqhkiG9w0BAQ0FADAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMCAXDTIyMDIyNTA0MTQIMFoY Dzk5OTkxMjMxMjMIOTU5WjAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMIICIjANBgkqhkiG9w0BAQ0FADAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMCAXDTIyMDIyNTA0MTQIMFoY Dzk5OTkxMjMxMjMIOTU5WjAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMIICIjANBgkqhkiG9w0BAQ0FADAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMCAXDTIyMDIyNTA0MTQIMFoY Dzk5OTkxMjMxMjMIOTU5WjAYMRYwFAYDVQQDDALsamwgU2VydmVyIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvCEYJfB7DEAW5jJzDL 0hrFwE9mkszrHrufQyg7gKi9nw/5/DrT54x+g2PRJapzCRcnsa2rpg4Qc2PHfYKQ/oqM6wxmVPGdjCa2sAImCGrn87ReaM3f1SHEhE4iVg7XKUMWB20hR+6S w1HKApY2AhUyutSTzrGx9Fcs8iFIMJIOYRnvj9QKMS92Ot2WIMDP7/ZIdjsGU1UCAm*zut00n/Wyym2txqjIYlsVWNIWv49luBzo590UZ5vrxJjDwkJV2VKV IlycEK+X7f9jAbCQo2vSSPHSwFVc5GdnjrPFKK0w+mil6cJSHk2ns/UW1bIzINOLPR3dLC5S0qHyF0b3bF9JT5kUS0H590UZ5vrxJjDwkJV2VKV V/b2aGn/yl5730cIzXWQuu/vXBABByseZESseMaaDUP3pl5IFDxxi5HkhladzJECAwEAAMMyDAwHQVDvR0BBFFN7lsXNGbbcVQLt6Xnf1vULteZIJuw Knwpyvf530eI/D0LogT4CQdbpHXKae/iqz0LDS8mhxUgBdwsf5r7tKq3t+RkLcCJiBwW0p6LZBwceRVP19T/9LU2Cv0JyM]voEuT0M2J3S029AVP2JsZ2g AlUdEwB/wQFMAMBAF8wQ0YJKOZIhvcNAQENBQADggIBAChe1fmL890yYdaUfW0gd8Noi0gHLGPTR9v2tEFbLOT/9Zuw6r3JiTMFrhrnJJ49xvtif60B7gL eax3Wcg0DD6yOsUUh2+S2E7CgT5X4MW1ZRdDLe0gZ/TNh6xb41Fuj5LXkFokBkoXyjuL+w0LIANVA2kylnjaE10MkRW2W9BU8grgmjyEv11dbvskBgws1T r83dU9a10hvZ6WE3pF9167_c07ypnx2v5ztUJM28ubet_JaFtHdEYJ0y0+RyJAox8WxeB3g2nZrfpMnNgxXveyLdPG8ylNaaE+ktY/2pJJ2Msbc/D4 IzcpdPhWSyubtO0jUuhdkc1R5024tEnTzqheFPDHAuTp+FE+fJ60QC1P2EJj4+A2bEkusyQMW0pnyn2Tv0ExoM2Yrk2Mytd6YwrDqGFuFoSLRrqr77 z3+rcoy4vwpw+1eHrwZdz/L8BNgwLdPfj058HZWATVSBNQKOrHDZ2D9nzcE50gve+sJMyvpD13J4H/5DHAJ7HVzDFJ2Wt+R24A	ATOR AOD 9w0Xdzpzbywwxb63kg1WegwbU0ITyhogkzZTrgCPT8GepAgmtKCTFXXt0/fzw1GrUefg1g0rTybgkhog1k023XZU/g1aaa1u3pk
cd4ufjzRtllocqczIW6ej8irtLnEjhro8vpl3Bt/83Nrjoklsire58wfwtpup3gINúvRcatZ0yg02fDvAcFi9B7fcWPxEnje44ClY= MIIE7jCCAtagAwIBAgIQAMlez5bMPpvTz/Ke8pvOATANBgkqhkiG9W0BAQOFADAYMRYwFAYDVQ0DDALsamwgU2VydmVyIENBMCAXDTyMDIyNTAOMTQIMFoY Dzk5oTkxMjMxMjMIOTUŠwjAyMRYwFAYDVQQDDALsamwgU2VydmVyIENBMCISUBgkqhkiG9W0BAQEFAAOCAg8AMIICcgKCAgEAvcEYJFB7DEAW9Ctku4NL Xvb/zoZpE0AxREzf0sa9wV-//5URdwfidNp6jn3quucWbJNdBikbxEcbDQ6QdINWnarXX63KK+7/7cSlUMLHEUxxEhgr705bBrIBQ7LEaXFJdImmCSjJzD/L OhrFwE9mkszrHruf0gyg7gKi9nw/5/prT54X+gZPRJapzCRcnsa2rpq4qc2PHfYKQ/oqM6wxmVPcdjCa2sAImCGrn87ReAM3fISHEhE4ivg7XkUMB26hR+65 WHKAPY2AhUyutSTzr63PEc8iFiMZ10YRnvj9QkMS92ot2WIMDP7/zIdjsGUUCAmVzut00n/Wyym2txqjIYlsVWNIW49IUBzo590U25vrxJjDwkJV2yKV IlycEK5+X7f9jAbCQoZvSSPHSwfvCsdEnjrPFK0Ww+mil6cJSHkZns/UymibZINoLP8jdL/L65S0qHyF0DsDF9JTsfuS9u+ScB6qHSmvpD94YW7UCTUZljuw KnwpyfS30eI/D0LogT4CqdbpHYKae/iq2QLDS8mhxUgBdwSf5r7tKq3t+RKLcCJiBwW0p6lZBwceRVP19T/0BUZ2v0yMlyOeIT0M2J3So22dNPZ3sZ2g AldEwE8/w0FMAMBAf8w0QYJKoZIhvcNAQEDBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL07/9ZwK6r3JJirMFrh7nJ349Xv1f60Br3gL eax3Wcg0DD6yOSUUH2+S2E7CgT5X4MW1ZRdDLe0gZ/TNh6xb41Fuj5LXkFokBkoXyjuL+w0LIANYA2kyJnjaE10MkRW2W1BUgRg0JyNiAaE+kYT/V2p/J2Mnsbc/D+ Zs6dPdNSyubt00jUuhdkc1R5o24tEnTzqheFPDHAUTp+FE+fJ6qUCIP22j4+AzbEkusyQMW0pnynZiv0ExcM2YrkZWtdf6Wn8QGTw6GgPIrooSLRrqq77 Z3+rCoy4vWwpw+1eHrwZdE/L93nxqz7ySoywLdPfjop58Hzw8Tx0SPNQK0rHDZ2D9nzCE5Dgve+s1MjzWhOp13j4H/SDHAJjRigkRaz4CrNw8QLinD4vsq	cYPK0PZ/+LvMBzqhkoIYdLRhIv9eibpnC5ckUCX+uwTXTTUCRXs+opsgrSJ2Sx5Y6ykdL2IL+57ELQIMWfsS0X5g7Db2oGHVGsFvSddVZkvEqQjVP1s/xUta
<pre>MIIE7jCCAtagAwIBAgIQAM1ez5bMPpvTz/ke8pv0ATANBgkqhki6g9w0BAQ0FabAixMRYwFAYDVQQDDA1samwgU2VydmVyIENBMCAXDTJyMDIyNTADMTQLMFoY Dzk5OTkxMjMXjM1oTU5WjAYMRYwFAYDVQQDDA1samwgU2VydmVyIENBMIICIjANBgkqhki6g9w0BAQEFAAOCAg8AMIICCgKCAgEAvCEYjBNTADAWQCtKu4NL Xvb/zoZpE0AxREzfosa9w4//SURGYTS4X+gZPRJapzCRcnsa2rpq4qc2PHfYKQ/oqM6wxmVPGdjCa2sAImCGrn87ReaM3f1SHEhE4ivg7XtuMWB26hRef6s w1HKApY2AhUyut5TzrGx9Fcs8iFlM2I0YRnvj96kMS9Zot2wIMbP7/zIdjsGUUCAmYzut00n/Wyym2txqjTYlsVwNlwv49luBzo590Uz5vrxjDwLV2VKV I1ycEK5+X7f9jAbCqozVs5PH5wfVc5denjrPFKOWw+mi16cJ5Hk2n5/UymibZINoLP8jdL/L65SoqHyF0b5DF9JTsfus9u+5C86qH5mvpD94yW7UCTu21juw Knwypvf530eI/O0LogT4CqdbpHYKae/iqz0LD58mhxUgBdWsf5r7tkg3t+RKLcCJiBwW0p61ZBwceRVP19T/08UZ0Zv0JyM1yOEuT0M2330229dNPZ3sA2g V/b2aGn/yl5739c1/sW0Wu/vXBABByszESseMaaDUP3p15HDxxi5HkhadzJECAwEAAAMMMDAHQVDVR00BBYEFN/15XNoEbvQLt6Kn71vUtecMaMA8G A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENB0ADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbLOT/9ZuW6r3IJirMFrh7nJ349xVtif60B7gL eax3Wcg0DD60yoSUUh2+52E7CgT5x4WW1ZRdDLe0gZ/TNh6xb41Fuj5LXkFokBkoXyjuL+w0LIANYA2ky1njaE10MkRW2wBU8grgmjyEv11dbu4SkBgws1T z83du9aq10hvZ0WE3pF9167c07ypnXvciztUJAFHHAUTDFFFF15GqUCLPE2Ij4+A2bEkusyQWW0pnn2Tv0ExoCM2Yrk2Wtd6SW1NAaE+kY1/V2p72Wth4Z4 Z3cq2Db9Kub003jUut0kc1R5o24tEnTzqheFDHAuTp+FE+f5GqUCLPE2Ij4+A2bEkusyQWW0pnn2Tv0ExoCM2Yrk2Wtd6SWTW9GGFIrooSLRrar77 z3+rCoy4vWwp+1eHrwZdE/L93nxqz7ySoywLdPfjop58Hv2MSspNQK0rHDZ2D9n2c5Dgve+s1MjzWh0Pp13j4H/5DHAJ7K1gk1gkmsc1m24A</pre>	cG4ufjZRt11ocqcZIW6ej8irtLnEjhr08vp13BT/83Nyj0klsire58wYwfvup3qINuVRcaTZ0yqo2fDvAcFj9B7TcWPxEnje44C1y=
<pre>xvb/zo2pE0AxREzf0sa9wV+//SURdwFidNp6jn1quucwbDNdBikbscbDQ6QdTNWnärXX63KK+7/7cslUMLHEUxxEhgr705bBTIBQ7LEaXfJdTmmCSjJ2DL 0hrFwE9mkszrHrufQyg7gKi9nW/5/DrT54X+g2PRJapzCRcnsa2rpq4Qc2PHfYKQ/oqM6wxmVPGdjCa2sAImCGrn87ReaM3fISHEhE4ivg7XKUMWB20hR45 WIHKAPV2AhUyutSTzr6x9FCs8iFIMZIOYRnvj9QkMS92ot2wIMDP7/zIdjsGUUCAmVzut00n/Wyym2txqjIYlsVWNLWV49luBzo590UZ5vrxJj0wkJV2yKV I1ycEk5+X7f9jAbCQoZvSSPHSwfVcSdEnjrPFK0ww+mil6cJSHk2n5/UymibZINoLP8jdL/L65S0qHyF0DSDF9JTsfus9u+ScB6qHSmvpD94Yv7UCTuZ1juw KnwypvfS30eI/D0LogT4CQdbpHYKae/iq2QLDS8mhxUgBdWsf5r7tKq3t+RKLcCJiBwW0p6lZBwceRVP19T/0BUZ0voJyMlyOEUT0V23SOZ9dXNPZ3sA2g V/b2a6n/y1S739cIsxWQwu/vXBABByseZESseMaaDUP3pl51FDxxiSHkLadzJECAwEAAMMDAwHQVDVR00BBVFEN/lsXNbbcvQLt6Xnf1vULtecMAMA8G A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAche1fmL80yydaUfWDgd8Noi0gHLGPTR9vztEFbL0T/9ZuW6r3IJirWF1h7nJ149xVtif60B7gL eax3Wcg0DD6yOsUUH2+S2E7CgT5x4Mw12RdDLeDgZ/TNh6xb41Fuj5LXkFokBkoxyjuL+w0LIANYA2ky1njaE10MkRw2wYBU8grgmjyEv111dbu4skBgws1 r83du9aqlohvZ6WE3pF9167c07ypnX2vc5ztUJMZ8UD+E/JaFth+dEYJ0yo+RyJAox8VAeB3QznZRfpMnNgxXvey1cMDG8yNiNaAE+kVT/V2p/J2Mnsbc/D+ Iz6gdPhWSyubt0ojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+fJ6QLCIPE2Ij4+AzbEkusyQMW0pnyn2Iv0ExoCM2Yrk2Mytd6Ywn9QT6wG6pIrooSLRrqr77 z3+rCoy4vWwp+1eHrwZdE/L93nxqz7ySQyuLdPfj0p58HzU8TXDSpNQK0rHDZ2D9nzCE5DgYe+s1MjzWh0PgH1YmgfTLFRh+GPv0Tpq9hr72Vvt+Nz4A</pre>	MIIE7jCCAtagAwIBAgIQAMleZ5bMPPvTZ/ke8pvOATANBgkqhkiG9w0BAQ0FADAYMRYwFAYDVQQDDA1samwgU2VydmVyIENBMCAXDTIyMDIyNTA0MTQ1MFoY
<pre>OhrFwE9mkszrHrufOyg7gki9nw/S/DrTS4X+G2PRjapzCRcnsa2rpq4qc2PHjfvKQ/oqM6wxmVPGdjCa2sAImCGrn87ReaM3f1SHEEfe4ivg7xKuMWB26hR46s w1HKApY2AhUyutSTrGx9FCs8iF1M2IOYRnvj9QkMS92Ot2w1MbP77zIdjsGU1UCAmYzut00n/Wyym2txqjIY1SVwN1Wv491uBzo590UZ5vrxjjDukJV2yKV I1ycEK5+X7f9jAbCqoZvSSPH5wfVcSdEqirPFKROw+mi16CjSHk2ns/Uym1bZ1NoLP8jdL/L65SoQHyF0DBSDF9JTsfus9u+SCB6qH5mvpD94Yw7UCTuz1juw KnwypvfS30e1/D0LogT4CQdbpHYKae/iqz0LDS8mhxUgBdwsf5rfKqJt+RkLcCJiBwW0p61ZBwceRVP19T/BUZ0ZvoJyM1yOEuT0M2J3SO29dXNPZJsA2g v/b2aGn/y1S739E1/sKWQWu/VXBABByseZESseMaaDUP3p151FDxxi5Hkh1adzJECAWEAAAMyMDAwHQ7DVR0BBYEFN/1sXNGbbcVQLt6KnF1vULtecMaMA8G A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbLOT/9ZuW6r3IJirMFrh7nJJ49xvtif60B7gL eax3Wcg0DD6y0sUUh2+S2E7CgT5x4WW1ZRdDLe0gZ/TNh6xb41Fuj5LXkFokBkoXyjuL+w0LIANYA2ky1njaE10MkRWZwYBU8grgmjyEv11dbusKBgws1T r83du9aq10hvZ6WE3pF9167c07ypnXzvc5ztUJW28uD+E7JaFth4EY30y0+RyJAox8WxAB3g2m2RfpMNngXxveyLoM58gV1hAaE+kYL7V2pJ2Mnsbc/D+ IzcgdPhWSyubt00jUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+f36qUC1PE2Ij4+AzbEkusyQMW0pnn2Tv0ExoCM2Yrk2Mytd6Ywn9QTGwGGpIrooSLRrqr77 z3+rCoy4vWwp+1eHrwZdE/L93nxqz7yS0ywLdPfj0p38HzU8RX8TXBSPNQK0rHDZ2D9nzCE5DgYe+s1MjzWvh0p13j4H/5DHAJjRigkRAz4CrNw8QL1inD4VwGc</pre>	DZK5OTKxMjMXMjM1OTU5WjAYMRYWFAYDVQQDDA1samwgU2VydmVyIENBMIICIjANBgkqhki69w0BAQEFAAOCAg8AMIICCgKCAgEAvCEYJfB7DEAW9CtKu4NL
wlHKApY2AhUyutSTzrGxÜFCs8iFlM2IOYRnvj0kMS92Ot2wIMbP77zIdjsGUlUCAmYzut00n/Wyym2txqjIYlsVWNlWv49luBzo590UZ5vrxJjDwkJV2yKV IlyCEK5+X7f9jAbCQozVsSPHSwfVCsdEnjrPFKOww+mil6cJSHk2ns/UymibZINoLP8jdL/L65SOqHyF0DsDF9JTsfus9u+SCB6qHSmvpD94YW/UCTuz1juw KnwppvfS3OeI/DOLogT4CQDbHYKae/iqzUDS8mhxUgBdWsf5r7tkg3t+RKLcCJiBWoD6jLBBwceRvP19T/oBUZOVoJyM1yOEUT0W2J3SO29dXPZJsA2g V/b2aGn/ylS739cIsxWQwu/vXBABByseZESseMaaDUP3p151FDxxi5Hkh1adzJECAWEAAAMYMDAwHQYDVR00BBYEFN/lsXNGbbcVQLt6Xnf1vULtecMaMA8G AlUdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9vztEFbLOT/9ZuW6r3JJirMFrh7nJ2H9xvtif60B7gL eax3Wcg0DD6yosUUhz+S2E7CgT5x4MW1ZRdDLe0gZ/TNH6kb41Fuj5LKKFokBkoXyjuL+w0L1ANYA2ky1njaE10MkRW2wFBW8grgmjyEv11Idbu4SkBgws17 r83du9aqlohvz6WE3pF91G7c07ypnX2vc5ztUJMZ8UD+E/JaFth+dEYJ0yo+RyJAox8VAeB3QznZRfpMnNgxXvey1CMDG8y1NiAaE+kYI/V2p/J2Mnsbc/D+ IzGpdPhWSyubt0ojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+fJ6QULIPEZIj4+A2bEkusyQMW0pny1Zv0ExoCM2YrkZMytd6Ywn9QTGwGGpIrooSLRrqr77 Z3+rCoy4vWwp+1eHrwZdE/L93nxqz7ySQyuLdPfj0p58HzU8TXDSpNQK0rHDZ2D9nzCE5DgYe+s1MjzW0hOPg+H1vmgfTLFRh+G+PovTpq9hr72Vvt+Nz4A	
<pre>IlycEk5+x7f9jAbCQoZvSSPHSwfvcSdEnjrPFkOww+mil6c3SHk2n5/UymibZINoLP8jdL/L65SbqHyF0D5DF9JTsfus9u+ScB6qHSmvpD94Yv7UcTuz1juw KnwpvfS3QeI/DOLogT4CQdbpHYKae/iqzQLDS8mhxUgBdwsf5r7tKq3t+RKLcCJiBwWOp6l2BwcRVP19T/oBUZOZvOJyM1yOEUM023SOZ9dXNPZJsA2g V/b2aGn/y1S739cIsxWQwu/vKBABByseZESseMaaDUP3p151FDxxiSHk1adz1ECAwEAAaMyMDaHQVDvRODBBVEFN/lsXN6bbcvQLt6Xnf1vUttecMaMA8G AlUdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbL0T/9ZwK6r3IJirMFrh7nJ149xvtif60B7gL eax3Wcg0DD6yOSUUH2+S2E7CgT5X4Mw12RdDLeDgZ/TNh6xb41Fuj5LxkFokBkoXyjuL+w0LIANYA2ky1njaE10MkRW2wYBU8grgmjyEv111dbu4SkBgws17 r83du9aqlohvZ6WE3pF91G7c07ypnX2vc5ztUJMZ8uD+E/JaFth+dEYJ0yo+RyJAoX8VAeB3QznZRfpMnNgXXveyLMDG8y1NiAaE+kYI/V2p/12Mnsbc/D+ Iz6gdPhWSyubt0ojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+f5GqULIPE2Ij4+AzbEkusyQMW0pnyn2Iv0ExoCMZYrk2Mytd6Ywn9QTGwG6pIrooSLRrqr7 z3+rCoy4vWwp+1eHrWZdE/L93nxqz7ySQyuLdPfjop58Hzu8TXDSpNQK0rHDZ2D9nzCE5DgYe+s1MjzWhOPgH1VmgfTLFRh+G+P0vTpq9hr72vt+xA4 EdPwDAex9X1/ugyL8aBNgHU0a35H+zoLI037azhK3wudRssgMvyjt6Qt0HB2FD9MU1YEw8J5ZsmS6q3WhyDpI3j4H/5DHAJjRigkRaz4Crnw8Q1inD4VwGc</pre>	ome we sinks zeneral (vyg.gk i snw/s) dri sek egzeko ab zeko acka zeneral v ku/ognow xinvega) CazsAink, Gena/ReamsTisHente41Vg/XKuMWB/b0hR4+05 wi Lukan Vahinatstra-cyGeC.gk je livitan v kukasta zeneral v kukasta zeneral v kukasta zeneral v kukasta zeneral
KnwppvfS30eI/D0LogT4CQdbpHYKae/iq20LDS8mhxUgBdwsf5r7tkg3t+RKLcCJiBwW0p61ZBwceRVP19T/08U20ZvoJyM1yOEuT0M2J3S029dXNPZJsA2g V/b2aGn/y1S739cIsXWQwu/vXBABByseZESseMaaDUP3p15IFDxxi5Hkh1adzJECAwEAAaMyMDAwHQVDvR00BBYEFN/IsXNGbbcVQLt6Xnf1vULtecMaMA8G AlUdEwEB/wQFMAMBAf8wQQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9vztEFbLOT/9ZuW6r3IJirMFrh/nJJ49xVtif60B7gL eax3Wcg0DD6yOsUUh2+S2E7CgT5x4Mw12RdDLe0gZ/TNh6xb41Fuj5LxKFokBkoXyjuL+w0LIANYA2ky1njaE10MkRwZwYBU8grgmjy£v11Idbu4SkBgws1T r83du9aq1ohvZ6WE3pF9167c07ypnx2Vc5ztUJW28uD+E/JaFth+dEYJ0yo+RyJAox8WxAB3QznzRFfbMNngxXveyLcMD63V1NiAaE+kYL7V2p/2Bmsbc/D+ IzGpdPhWSyubtoojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+fJ6qUC1PE2Ij4+A2bEkusyQMW0pnyn2Iv0ExoCM2Yrk2Mytd6Ywn9QTGwG6pIrooSLRrqr77 z3+rCoy4vWwpw+1eHrwZdE/L93nxqz7yS0ywLdPfjop38HzU8TXDSPMQKOrHDz2D9nzcE5DgYe+s1DjzwhOPDg1HlrgHTLFRh+G+POvTpq9hr72Vwt+Az4A	Winepitzanoy desize o system in zero kni y soka system in zero za sobio cani zero o na mizero na zero sobio zverzi je na zero kni y soka system i na zero kni y soka zero za sobio zverzi je na zero kni zero kni zero kni zero kni zero za sobio zverzi zero zero zero zero zero zero zero zero
V/b2aGn/y1S739cIsXWQwU/vXBABByse2ESseMaaDUP3p151FDxxi5Hkh1adzJECAWEAAaMyMDAwHQYDVROOBBYEFN/1sXNGbbcVQLt6Xnf1vULtecMaMA8G A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvCNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbLOT/9ZuW6r3IJirMFrh/nJ2H3vtif60B7gL eax3Wcg0DD6yOsUUhz+S2E7CgT5X4MW1ZRdDLe0gZ/TNR6kb41Fuj5LXkFokBkoXyjuL+wOLLANYA2ky1njaE10MkRW2WBU8grgmjyEv11Idbu4SkBgws1T r83du9aqlohVz6WE3pF91G7c07ypnX2vc5ztUJMZ8UD+E/JaFth+dEYJ0yo+RyJAox8VAeB3QznZRfpMnNgxXvey1cMDG8y1NiAaE+kYI/V2p/J2Mnsbc/D+ IzGpdPhWSyubt0ojUuhdkc1R5o24tEnTzgheFPDHAuTp+FE+fj6QULIPEZIj4+A2bEkusyQMW0pnyn2Iv0ExoCM2Yrk2Mytd6Ywn9QTGwGGpIrooSLRrqr77 z3+rCoy4vWwpw+1eHrwZdE/L93nxqz7ySQyuLdPfjop58Hzu8TxDSpNQK0rHDz2D9nzCE5DgYe+s1MjzW0hOPg+H1vmgfTLFRh+G+POvTpq9hr72Vwt+Nz4A EdPw0Aex9X1/ugyL8aBNgHU0a35H+zoLIo37azhK3wudRssqMvyjt6Qt0h8BfP5pdW1YEw8J5ZsmS6G3WhyDpI3j4H/5DHAJjRigkRaz4Crnw8QLinD4VwGc	Knwypy f S30eI/D0LogT4C0dbpHYKae/ig20LDS8mhXUgBdwsf5r7tKg3t+RKLcC1iBwW0p61ZBwceRVP19T/oBU202Vo1w1V0FuT0W713S072dxNP21sa2a
A1UdEwEB7woFMAMBAf8wDQiytozIhvcNAQENBQADggIBAChelfmL890yYdaUfWDgd8NoiOgHLGPTR9VztEFbLOT/9ZiwG6r3IJirMFrh7nJ149xttif60B7gL eax3Wcg0DDGiyOSUUhZ+S2E7CgT5X4MWl2RdDLeDgZ/TNh6xb41Fuj5LXkFokBkoXyjuL+WOLIANYAZkylnjaE1OMkRw2wYBU8grgmjyEv11Idbu4SkBgw51T r83du9aqlohvz6WE3pF91G7c07ypnX2vc5ztUJMZ8UD+E/JaFth+dEYJ0yo+RyJAoxBVAeB3cznZRfpMnNgXxveyLCMDG8ylNiAaE+kYI/V2p/2ZMnsbc/D+ IzcgpdPhWSyubtoojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+fJ6qUCLPE2Ij4+A2bEkusyQMW0pnyn2Iv0ExoCMZYrk2Mytd6Ywn9QT6wGGpIrooSLRrqr7 z3+rCoy4vWwpw+1eHrWZdE/L93nxqz7ySQywLdPfjop58HzU8TXD5PNQK0rHDZ2D9nzcE5DgYe+s1MjzWOhOPg+H1vmgfTLFRh+G+POvTpq9hr72VWt+Nz4A EdPw0Aex9X1/ugyL8ABNgMU0a35H+zoLIO37azhK3wudRssqMvyjt6Qt0HB8FP5pdWlYEw8J5ZsmS6G3WhyDpI3j4H/5DHAJjRigkRaz4CrNw8QlinD4VwGc	V/b2aGn/y1S739cIsxWQwu/vXBABByseZESseMaaDUP3p151FDxxi5Hkh1adzJECAwEAAaMyMDAwHQYDVR00BBYEFN/1sXNGbbcVQLt6Xnf1vULtecMaMA8G
r83du9āqlohvz6WE3pF9lG7c07ypnX2vc5ztUJMŽ8uD+E/JaFth+dEYJOyo+RyJAoxBVAeB3QznZRfpMnNgxXvey1cMDG8ylNiAāE+ŔYI/V2p/J2Mns6c/D+ IzGpdPhWSyubtoojUuhdkc1R5o24tEnTzqheFPDHAuTp+FE+fj6qUlPE2Ij4+AzbEkusyQMW0pnyn2Iv0ExoCM2Yrk2Mytd6Ywn9QTGwGGpIrooSLRrqr77 Z3+rCoy4vWwpw+leHrwZdE/L93nxqz7ySQywLdPfjop58HzU8TxDspNQK0rHDZ2D9nzCE5DgYe+s1MjzW0hOPg+H1vmgfTLFRh+G+POvTpq9hr72vWt+Nz4A EdPwOAex9X1/ugyL8aBNgMU0a35H+zoLIo37azhK3wudRssqMvyjt6QtOh8BfP5pdWlYEw8J5ZsmS6G3WhyDpI3j4H/5DHAJjRigKRaz4Crwk8QtinD4VwGc	A1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQENBQADggIBAChe1fmL890yYdaUfWDgd8Noi0gHLGPTR9VztEFbLOT/9ZuW6r3IJirMFrh7nJJ49xVtif60B7gL
IzGpdPhWSyubtoojUuhdkclR5o24tEnTzqheFPDHAuTp+FE+f5GqUCIPE2Ij4+A2bEkusyQMW0pnyn2Iv0ExoCM2Yrk2Mytd6Ywn9QTGwGGpIrooSLRrqr77 Z3+rCoy4vWwpw+1eHrWZdE/L93nxqz7ySQywLdPfjop58Hzu8TXDSpNQK0rHDZ2D9nzCE5DgYe+s1MjzWOhOPg+H1vmgfTLFRh+G+POvTpq9hr72VWt+Nz4A EdPwDAex9X1/ugyL8aBNgMUDa35H+zoLIo37azhK3wudRssqMvyjt6QtOh8BfP5pdW1YEw8J5Z5mS6G3WhyDpI3j4H/5DHAJjRigkRaz4CrNw8QlinD4VwGc	eax3wcg0DD6y0sUUhZ+S2E7CgT5x4Mwl2RdDLeDgZ/TNh6xb41Fuj5LxkFokBkoXyjuL+w0LIANYA2kylnjaE10MkRw2wYBU8grgmjyEvl1Idbu4SkBgwsĨT
Z3+rCoy4vWwpw+1eHrWZdE/L93nxqz7ySQywLdPfjop58HZu8TXDSpNQKOrHDZ2D9nzCE5DgYe+s1MjzWOhOPg+H1vmgfTLFRh+G+POvTpq9hr72vWt+nz4A EdPwOAex9x1/ugyL8aBNgMUOa35H+zoLIo37azhK3wudRssqMvyjt6QtOh8BfP5pdW1YEw8J5ZSmS6q3WhyDpI3j4H/5DHAJjRigkRAz4CrNw8Q1inD4VwGc	r83du9aq1ohVz6WE3pF9IG/c0/ypmX2vc5ztUJMZ8uD+E/JaFth+dEYJ0yo+RyJAoxBVAeB30znZRfpMnNgxXvey1cMD68y1NiAaE+kYI/V2p/J2Mnsbc/D+
EdPw0Aex9x1/ugyL8aBNgMU0a35H+zoLIo37azhK3wudRssqMvyjt6Qt0h8BfP5pdW1YEw8J5ZSmS6q3WhyDpI3j4H/5DHAJjRigkRAz4CrNw8Q1inD4VwGc	12GpdPhwSyubtOojUuhakcTR3o24EEnT2qhePDHAuTp+E+t35q0UCTPE21j4+A2bEkusyQMWUpnyn2IvUExoCM2VrkZMytd6Ywm90TGwG6pIrooSLRrqr/7
	23+FC0949WmpH1EHTW2dz/L95DXd279SQWLdPTJ0p36H2d6TXD5PN0KUPHD2ZD9h2CE3DgYe4SIMj2W0h0Pg+H1VmgTTLFRH-G+P0vTpq9hr/2VWE4P4A EdwoAse9VJ1/umg148_8NiAMW035UL321To373+bY3wpdPc3mhy2i+66F0BR6P554WJV5W3575mc6637W4mpo73i4i/5puta15i4abn2464chy80

ADDITIONAL TOOLS

Once TAC-040 achieved persistence. Deepwatch observed that TAC-040 employed various publicly available open-source tools cloned from GitHub [T1588.002] (listed below). In addition, Deepwatch observed one toolset, CrackMapExec (figure 6), which serves as an attack framework with multiple tools. A security solution the victim had deployed flagged this framework as malicious.

One of these <u>CrackMapExec</u> (Figure 7) tools was used to conduct Kerberoasting [T1558.003] and AS-REP Roasting [T1558.004]. However, we could not recover the contents of the output file (output.txt), so we can not confirm if this attempt was successful. However, we do not have evidence suggesting the threat actor was able to move laterally within the network before the compromised server was brought offline.

git.exe clone --recursive https://github.com/byt3bl33d3r/CrackMapExec

Figure 8: Cloning CrackMapExec from GitHub

Additionally, TAC-040 attempted password spraying [T1110.003] on numerous accounts but failed. Furthermore, the threat actor(s) attempted to join a computer to the domain using 1.py.

Analyst Note

Initial tool ingress was likely achieved by an, as yet, undetermined method to maintain access independent of the Confluence vulnerability. Deepwatch did not observe dropper or download commands that would have allowed the threat actor to download tools that would allow them to remove their dependency on Confluence for access. Yet, the later portion of the attack TAC-040 carried out did not have a parent process of tomcat9. exe, indicating there was direct access without the need to re-exploit Confluence or utilize a webshell in the installation directory.

TAC-040 demonstrated the ability to upload custom tools (all.exe and dump.dll) through an unknown method than running a traditional download cradle with the Confluence RCE vulnerability.

ADDITIONAL TOOLS

- ✓ Open-source tools cloned from GitHub:
- NetRipper
- PowerSploit
- Invoke-Vnc
- CME-PowerShell-Scripts
- CrackMapExec: attack framework with multiple tools
- Invoke-Obfuscation
- SessionGopher
- mimipenguin
- mimikittenz
- RID_Hijacking
- RandomPS-Scripts

During our investigation into this incident, a loader for an XMRig crypto-miner was observed in the forensic artifacts. Deepwatch's technical analysis of this loader with associated observables can be read in <u>part 3</u> of this threat report.

Analyst Note

Deepwatch assesses that the XMRig related artifacts could be the result of multiple threat actors based on known threat actor activity related to cryptominers.

EXFILTRATING SENSITIVE DATA

Network logs suggest around 700MBs of data was exfiltrated [T1567] to a Linode server (192.46.223[.]211) [T1583.003].

Analyst Note

Based on the directories, folders, and files archived, exfiltrated data likely included an archive of the Active Directory, web configuration files, network hosts, C drive log files, and other sensitive data. However, we cannot positively confirm which archived files TAC-040 exfiltrated due to visibility gaps.



What You Need to Do

For organizations unable to upgrade Confluence immediately, Atlassian has provided a temporary workaround for the following specific product versions.

- Confluence 7.15.0 7.18.0
- Confluence 7.0.0 Confluence 7.14.2

Additional risk reduction recommendations include:

- Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.
- · When PowerShell is necessary, restrict PowerShell execution policy to only administrators that require it.
- · Where possible, only permit the execution of signed scripts.
- Set account lockout policies after five to 10 failed login attempts to prevent passwords from being guessed and enforce multifactor authentication.
- Make sure that all accounts have Kerberos pre-authentication enabled whenever possible and audit changes to settings.
- · Restrict access to Confluence only when a user has been authenticated or only allows access from trusted sources.
- Segment Systems that are Internet exposed from the internal network to limit the impact of internal systems from being compromised.
- Ensure proper systems/applications inventory is regularly occurring, especially Internet-facing ones, for identification of systems/applications to include in a patch management program.
- Implement a patch management program with critical priority patching for systems/applications that are Internet-facing.

Observing this activity cluster may be possible by auditing and monitoring logs for the following:

- · Bash, cmd.exe, or powershell.exe spawned by Apache Tomcat.
- .jsp, .jar. .asp, .aspx, or .php files being created or modified in Confluence/Bitbucket/Jira web directories.
 - It may also be possible to detect webshell installation artifacts in confluence_install_dir\work\Standalone\localhost\ ROOT\org\apache\jsp\ with the naming convention NAME_jsp.java for .jsp webshells that have already been deleted.
- Unexpected service installation activity (especially those that launch .exe files in the Logs or Temp directories).
- · Git clone activity and associated DNS queries/proxy logs.
- Files with short names being executed (ex. 5.exe, ad.exe).
- Executables run multiple times with a high distinct count of source paths.

• Ex. rar.exe being run in C:\Temp, C:\Logs, and C:\Web.

- Usage of the following Live Off the Land Binaries (LOLBins): reg, net, or whoami, spawned as child processes of Apache Tomcat (Event ID 4688).
- rar.exe or 7z.exe activity on Windows and related commands on Linux
 - Especially when running in succession in multiple configuration directories or paths containing other sensitive data

Intelligence Gaps

Regarding this activity cluster, there are still a few unanswered questions. First and foremost, we cannot be certain of TAC-040's intentions and goals due to visibility gaps. However, it is likely that TAC-040's goal was espionage-related. However, we can not completely rule out that they were financially motivated. The Threat Intel Team needs additional evidence to build confidence in this hypothesis.

Secondly, the threat actor likely exploited CVE-2022-26134. However, there are other vulnerabilities, albeit unlikely, that the actor could have exploited. Unfortunately, visibility gaps prevent us from confirming which vulnerability TAC-040 exploited.

Thirdly, we could not recover many tools, and scripts dropped on the server by TAC-040 or determine how they were dropped. Therefore, we are unable to assess their purpose and capabilities.

Conclusion

TAC-040 highly likely exploited CVE-2022-26134 in an outdated Confluence server, highlighting the importance for organizations to apply patches as soon as possible and ensure that systems and servers that contain sensitive information are not exposed to the internet. One item to note is that TAC-040 created or had access to a never-before-seen backdoor, which we analyzed in <u>Part 2</u> of this report.

> Additionally, TAC-040 archived the Active Directory and several sensitive files and cloned numerous tools from GitHub. Targeting a non-profit research organization, archiving of Active Directory, registry hives, and the suspected contents of other sensitive files suggest that TAC-040 may have an espionage mandate. However, we can not completely rule out that they may be financially motivated.

Therefore, organizations that conduct research in healthcare, education, international development, and environmental and agriculture or provide technical services in these areas are likely targets of this threat actor. However, organizations in other sectors that operate in these areas may also be targets.

Deepwatch immediately alerts customers when new threats occur or who have been targeted or attacked, giving them the tools and actionable intelligence they need to safeguard their environments. We encourage organizations to share our threat intelligence reports with other teams or colleagues, including our weekly Cyber Intel Briefs and Customer Advisories.

Deepwatch Threat Intel Team has moderate assurance in our overall analysis of this threat. The data is sourced from our internal collections. However, no additional corroborating sources were available for the assessment, and analysts' estimations are based on available data. Furthermore, the analytic task was moderately complex, and analysts' collaborated and employed a few structured analytical techniques and were afforded sufficient time to complete the analysis.

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from everincreasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's fastest, most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

Visit www.deepwatch.com to learn more.

CONTACT US

4030 W Boy Scout Blvd, Suite 550 Tampa, FL 33607 (855) 303-3033

MITRE ATT&CK

T1583.003	Acquire Infrastructure: Virtual Private Server	T1560.001	Archive Collected Data: Archive via Utility
T1588.006	Obtain Capabilities: Vulnerabilities	T1110.003	Brute Force: Password Spraying
T1588.002	Obtain Capabilities: Tool	T1543.003	Create or Modify System Process: Windows Service
T1587.001	Develop Capabilities: Malware	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting
T1190	Exploit Public-Facing Application	T1558.004	Steal or Forge Kerberos Tickets: AS-REP Roasting
T1033	System Owner/User Discovery	T1567	Exfiltration Over Web Service
T1119	Automated Collection		

Observables

Note: Observables are properties (such as an IP address, MD5 hash, or the value of a registry key) or measurable events (such as creating a registry key or a user) and are not indicators of compromise. The observables listed below are intended to provide contextual information only. Deepwatch evaluates the observables and applies those it deems appropriate to our detections.

Observing sets of these properties (observables) could indicate compromise. For instance, observing an IP address, the creation of a user with admin privileges, and a registry key could be indicators of compromise and should be investigated further.

Webshell (jquery.aspx)

SHA256: 3fe094bab0e6c93a9a99a2dce75c60c5f3526ac786bb8b551534f098fa1419d3

1.py

SHA256: cbea88a0fcef3a157ca83582f152e3a67257c6de22ecdda025db78d94dead1c1 nb exe

SHA256: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

wab.exe (ljl Backdoor)

SHA256: 112d5f4755154d7b1ac6f5c0c84a2b0dfb053bd6c308e23dfd96b9206f105e40

wab32res.dll (ljl Backdoor) SHA256: f2dfe17f992072266ac57835432b56834657ea0e75eb42fb9a034b3e517f3e25

Linode Server 192.46.223[.]211

IP that communicated with nb.exe 205.185.121[.]53 (Frantech)

Files and Commands Executed by TAC-040:

- c:\users\public\all.exe
- c:\users\public\dump.dll
- c:\Windows\System32\query.exe user
- c:\Windows\System32\cmd.exe /c "cd /d "C:\Windows\system32\"&c:\users\public\rar.exe a
- c:\users\public\d.rar c:\users\public\1.bin"
- c:\Windows\System32\PING.EXE www.google.com
- c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe echo ((new-object Net.Sockets.TcpClient).Connect(\"INTERNAL_IP\",636)) "open!"
- c:\Windows\System32\cmd.exe /c "cd /d "C:\Windows\system32\"&ping -n 1 HOSTNAME"
- c:\Windows\System32\cmd.exe /c "cd /d "C:\logs\t"Samp;"C:\Program Files\7-Zip\7z.exe" -t7z a 1.7z .*.hiv -mx9"
- c:\Windows\System32\net.exe user USER /domain
- c:\ProgramData\Git\DATE\mbae-svc.exe kerberoast /domain:DOMAIN /dc:HOSTNAME /outfile:1.txt
- c:\Windows\System32\cmd.exe /c "cd /d "C:\Windows\system32\"&net view \\HOSTNAME"
- c:\Windows\System32\cmd.exe /c "cd /d "C:\Windows\system32\"&net group "Enterprise Key Admins" /domain"
- c:\logs\DrSDKCaller.exe
- c:\Windows\System32\sc.exe create "VBoxxSDS" binpath= "C:\logs\DrSDKCaller.exe" type= share start= auto displayname= "VirtualBox system service" depend= Tcpip
- c:\logs\Python39\python.exe 1.pyá-dc "HOSTNAME" -dc-ip "INTERNAL_IP" -computer-name "HOSTNAME" FILE_NAME.ns/ USER:"PASSWORD"
- C:\Windows\System32\cmd.exe /c "cd /d "C:\logs"&for /l %b in (1,1,255) do ping x.x.x.%b -n 1 >>t.txt"
- C:\Windows\System32\cmd.exe /c "cd /d "C:\Windows\system32\"&net localgroup administrators"
- C:\PerfLogs\magick.exe -I tcp -p 445,443 INTERNAL_SUBNET
- "C:\logs\Python39\python.exe" "C:\logs\Python39\Scripts\pipx.exe" install crackmapexec