CYBER INTELLIGENCE IN PROTECTING ORGANIZATIONS FROM MALICIOUS ACTIVITY

Viktor V. Lilov, Ekaterina M. Konstantinova, Tsvetoslav S. Tsankov

[1] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Student, solaviki@abv.bg
[2] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Student, katminkova2@gmail.com
[3] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Assoc. prof. Eng., PhD, c.cankov@shu.bg

***Abstract**: Many organizations put great effort and resources into protecting their information from malicious activity. Anti-cybercrime departments are being set up, software is being bought, but this makes their companies even more attractive to criminals. The report reveals some of the modern countermeasures that should be useful to all users.*

***Keywords**: Cybersecurity, Cyber spying, EternalBlue, Threat intelligence, WannaCry*

КИБЕРРАЗУЗНАВАНЕТО ПРИ ЗАЩИТАТА НА ОРГАНИЗАЦИИТЕ ОТ ЗЛОУМИШЛЕНИ ДЕЙСТВИЯ

Виктор В. Лилов, Екатерина М. Константинова, Цветослав С. Цанков

Въведение

Според Microsoft Lean on the Machine, големите средностатистически организации всяка седмица трябва да преглеждат 17 000 предупреждения за вредни програми. Селектирането трябва да бъде на ниво център за управление на мрежата, а забавянията могат да доведат до ефекта на доминото, т.к. ако на това ниво се получи отказ, операцията също ще приключи неуспешно и ще трябва да се предаде на екипа за реагиране на компютърни инциденти [1], [3].

За предотвратяването на заплахите в САЩ например е предвидено Управление на разузнаването и анализ, което използва разузнаване за повишаване на сигурността. Това разбира се е за сметка на информационен обмен между редица учреждения и изготвянето на прогнози, предоставяни на лица, които трябва да вземат решения на всякакви нива. Узнаването на мотивите и методите, които използва противника е от първостепенно значение за откриването на злоумишлени действия с помощта на обичайни сензори.

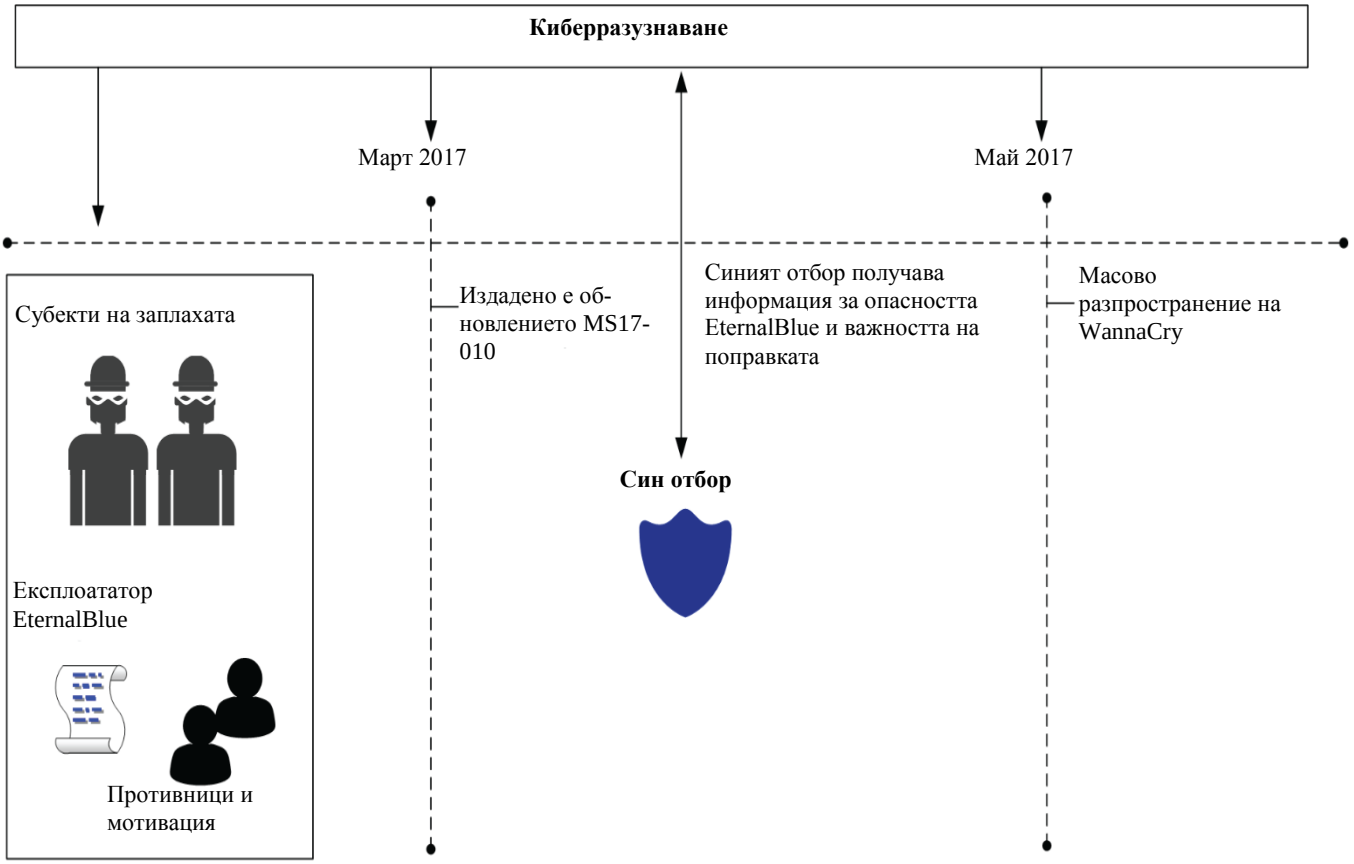
Мотивацията на противника може да разкрие неговия профил, който може да бъде:

- киберпрестъпник – неговата основна мотивация е получаването на финансов резултат;
- хактивист – при тях е по-широк спектъра на мотивация, като може да се изразява в политически пристрастия или каквито и да е случайни причини;
- кибершпионин на държавно ниво – макар че болшинството такива случаи са в частния сектор, те по същия начин се вмъкват и в големите държавни компании.

Така според дейността на компанията може да се предвиди очаквания профил на злосторника, който си я е набелязал като цел.

WannaCry

Масово разпространение на програмата-изнемогвател WannaCry е било в петък, на 12 май 2017 г. WannaCry е работила с програмата-експлоататор EternalBlue, която е експлоатирала уязвимости в протокола Server Message Block (SMB) v1 (CVE-2017-0143) на Microsoft. В отговор на това, на 14 март 2017 г., почти два месеца преди разпространението на WannaCry, Microsoft издава поправка на уязвимостта (фиг. 1) [5], [6].



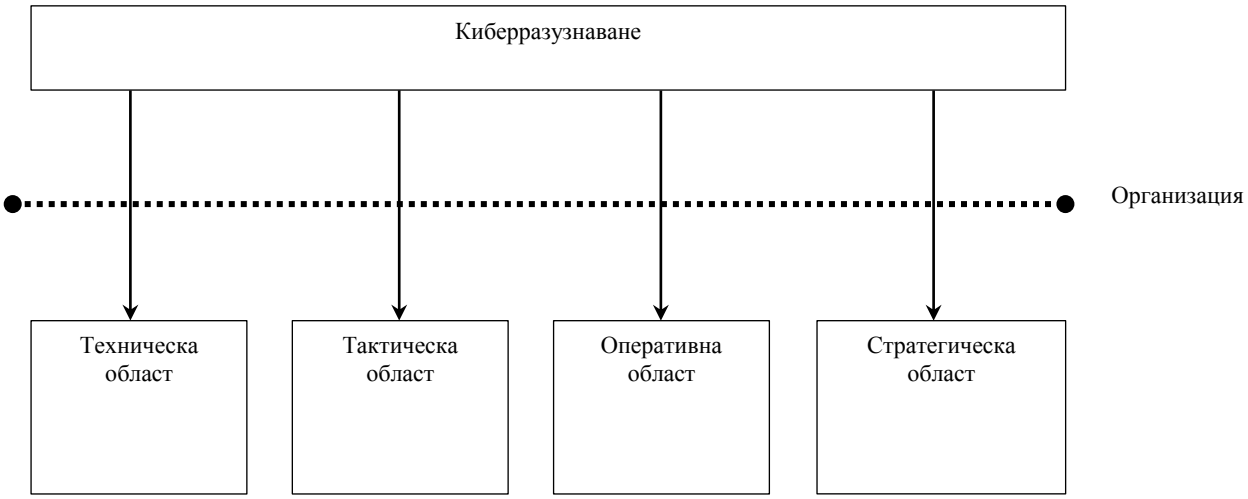
Фиг. 1: Опит за предпазване от WannaCry

Благодарение на хакерската група The Shadow Brokers, киберразузнаването получава информация за заплахата още на ранен стадий, когато EternalBlue едва се е появил в мрежата. Членовете на групата са били познати от предишни злодеяния. Като се знаят техните мотиви, както и начина на работа на EternalBlue, се изчаква поправката от Microsoft, за да се защитят компаниите.

Много организации не са осъзнавали проблема до край и вместо поправките, просто са отключвали достъп от интернет по SMB протокол. И макар че това е бил приемлив ход, той не е

отстранил основната причина. Така през юни 2017 г. се е разпространил масово още един вирус-изнемогвател – Petya. Petya е използвал EternalBlue за по-нататъшно разпространение по мрежата. Така при компрометирането на един компютър от вътрешната мрежа, той се приготвя да експлоатира други, на които не е инсталирана поправката MS17-010.

Знаейки своите противници, специалистите могат да предприемат по-ефективни решения за защита на ресурсите. Киберразузнаването не трябва да се разглежда като инструмент на информационната безопасност, макар че тя влиза в нейните граници. Киберразузнаването трябва да е инструмент, спомагащ за вземането на решения по защитата на организациите. Информацията, която се получава при киберразузнаването може да се използва в различни области, като по такъв начин правилното използване на киберразузнаването оказва пряко влияние на цялата организация (фиг. 2) [1], [8].



Фиг. 2: Области използващи киберразузнаването

Организациите използващи локални или облачни продукти от Microsoft, могат да се чувстват в безопасност, т.к. софтуерният гигант им предоставя средства за киберразузнаване, включени в тези продукти. Това става благодарение на предимствата от общото киберразузнаване, които Microsoft използва по различни канали, т.напр.:

- Microsoft Threat Intelligence Center, който обединява данни от:
  - Honeypot, вредоносни IP-адреси, ботнетове и обобщения за зловреден софтуер;
  - странични източници, обобщаващи данни за заплахи;
  - наблюдения и събиране на разузнавателни данни;
- интелект, добиван от употребата на услугите от Microsoft;
- данни за заплахи, обобщавани от Microsoft и трети лица.

Microsoft интегрира резултатите в своите продукти, т.напр. в Windows Defender Advanced Threat Protection, Център за безопасност Azure, Office 365 Threat Intelligence, Cloud App Security и др.

Киберразузнаването в помощ на разследванията

Киберразузнаването е крайно необходимо при разследванията на подозрителните злоумишлени дейности. Въпреки че Синият отбор работи като главен над системата за защита, тя сътрудничи с групата за реагиране на компютърни инциденти, предоставяйки й важни данни, които могат да помогнат за намирането на основната причина за проблемите.

Единствената цел за реагиране на инцидент не е само знанието за компрометираната система. В края на разследването трябва да се отговори на няколко въпроса:

- Какви системи са били компрометирани?
- Къде е започнала атаката?
- Кой потребителски идентификатор е използван за започване на атаката?
- Имало ли е фронт за по-нататъшно разпространение по мрежата?
  - Ако да, то какви системи участват в това разпространение?
- Имало ли е място с по-големи привилегии?
  - Ако да, то кой потребителски идентификатор е бил компрометиран?
- Правен ли е опит за връзка с командно-контролния сървър?
- Ако да, имал ли е успех опита?
  - Ако да, изтеглено ли е нещо оттам?
  - Ако да, изпратено ли е нещо оттам?
- Предприет ли е опит за избавяне от уликите?
  - Ако да, имал ли е успех опита?

Тези съществени въпроси могат да помогнат за успешната работа и увереността, че заплахата е напълно локализирана и изтрита от средата [3], [4], [7].

За отговорите на повечето от тези въпроси е възможно използването на функцията за разследване на Центъра за безопасност. Тази функция позволява да се проследи пътя на атаката, задействаните потребителски идентификатори, компрометираните системи и осъществените злоумишлени действия.

Киберразследване

В много случаи специалистите могат да бъдат подведени, че има проблем, който е свързан с безопасността. При събиране на повече данни и по отговорите на поставените въпроси, всеки ще направи преценка за мащабите на проблема. Затова от особена важност е първоначалното сортиране за хода на разследването. Ако няма реални доказателства за проблем с безопасността, а просто оплаквания с намалена производителност, то следва да се отстранят проблемите по бързодействието, а не веднага да се алармират отрядите за реагиране. Трябва да има пълна съгласуваност между IT-отдел, Оперативен отдел и Отдел за безопасност, за да не се натоварват излишно със задачи, които са към друга поддръжка [6], [8].

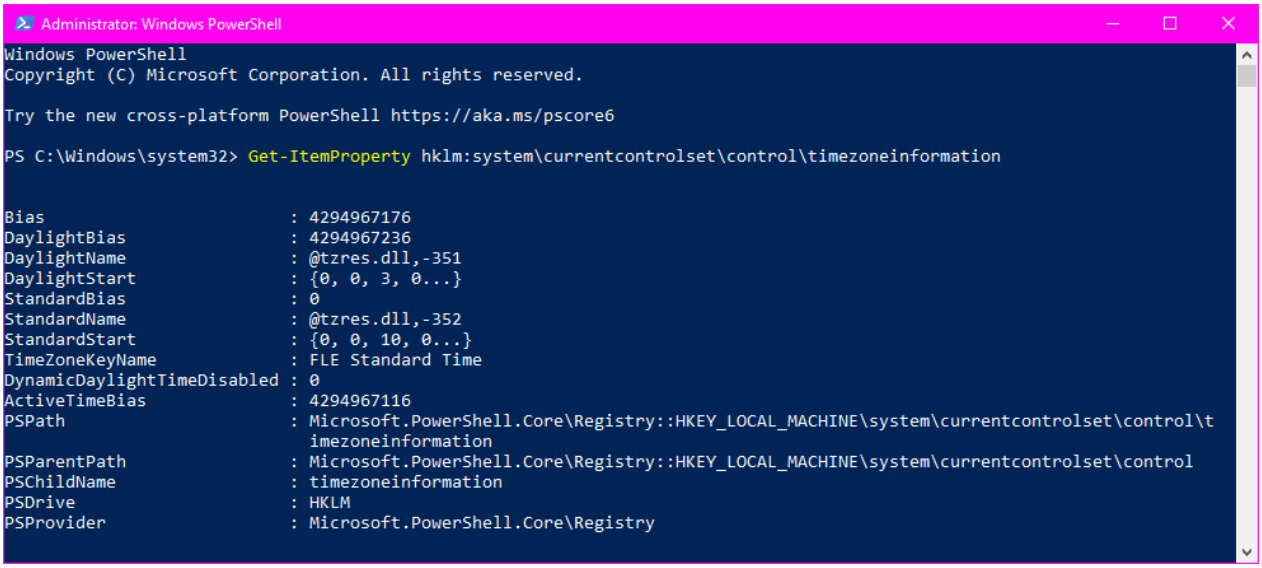
При първоначален разбор е важно определянето на честотата на възникване на проблемите. Ако проблема не е в настояще време, налага се да се настрои средата за събиране на данни, когато проблема ще се прояви. За крайния потребител се съставя план за действие в стъпки. Успехът от разследването ще зависи от качеството на събраните данни.

В реално време постъпват много данни, но при събирането им трябва да се съсредоточим само върху жизненоважните и значещи артефакти от системата, която е цел на разследването. Голямото количество данни не води до подобряване на разследването, дори напротив, може да ни отдалечи от основната причина за проблема.

Когато се работи с глобални организации, които имат устройства в цял свят, трябва да се знае часовия пояс в който работи системата, която е цел на разследването. В Windows тя е записана в ключ на регистъра:

```
HKEY_LOCAL_MACHINE\SYSTEM\Current-ControlSet\Control\TimeZoneInformation
```

За получаването на информацията може да се използва командата `Get-ItemProperty` в Windows PowerShell (фиг. 3).



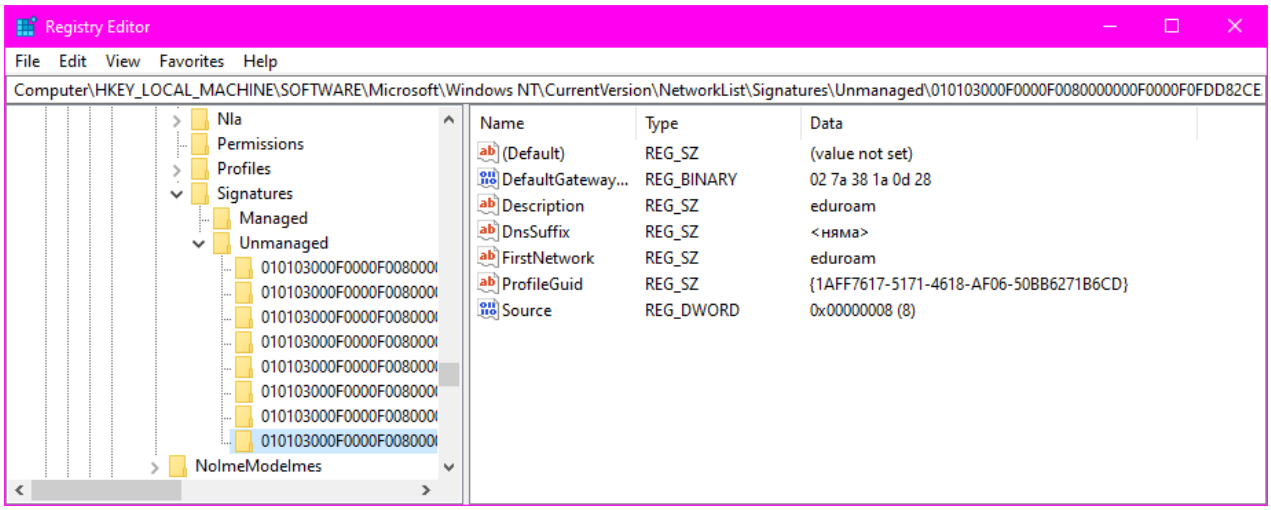
Фиг. 3: Информация за часовия пояс

Обръща се внимание на TimeZoneKeyName: FLE Standard Time, като данните трябва да са актуални, когато се започва анализиране на файлове и корелация на данни [2], [5].

Друг важен ключ на регистъра е за получаване на информация за мрежата:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged and Managed`

Тези раздели показват мрежите, към които е включван дадения компютър. Едни от резултатите на ключа `unmanaged` са дадени на фиг. 4.



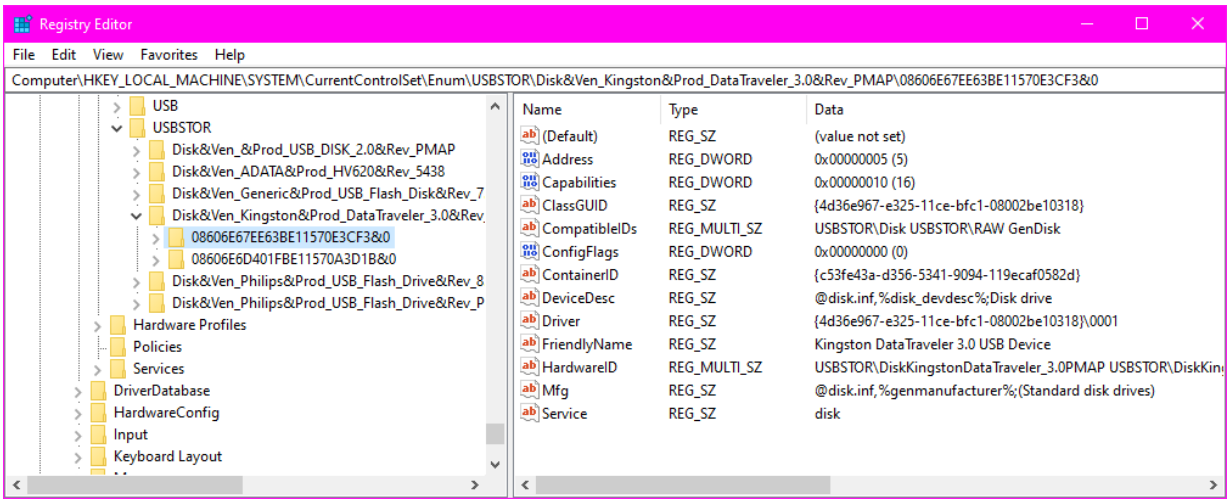
Фиг. 4: Данни за мрежа от списъка Unmanaged

Изложените два артефакта са часовия пояс и мрежите, които компютъра е посетил. Това е от особено значение за устройства, които се използват от персонала за работа извън фирмата, например преносими компютри и таблети [5], [7].

В зависимост от изследваните проблеми, трябва да бъде проверено и използването на USB устройствата на изследвания компютър. Това е видно в ключовете на регистъра:

`HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` и
`HKLM\SYSTEM\CurrentControlSet\Enum\USB`

Данните за едно такова устройство са показани на фиг. 5.



Фиг. 5: Данни за използвана USB памет

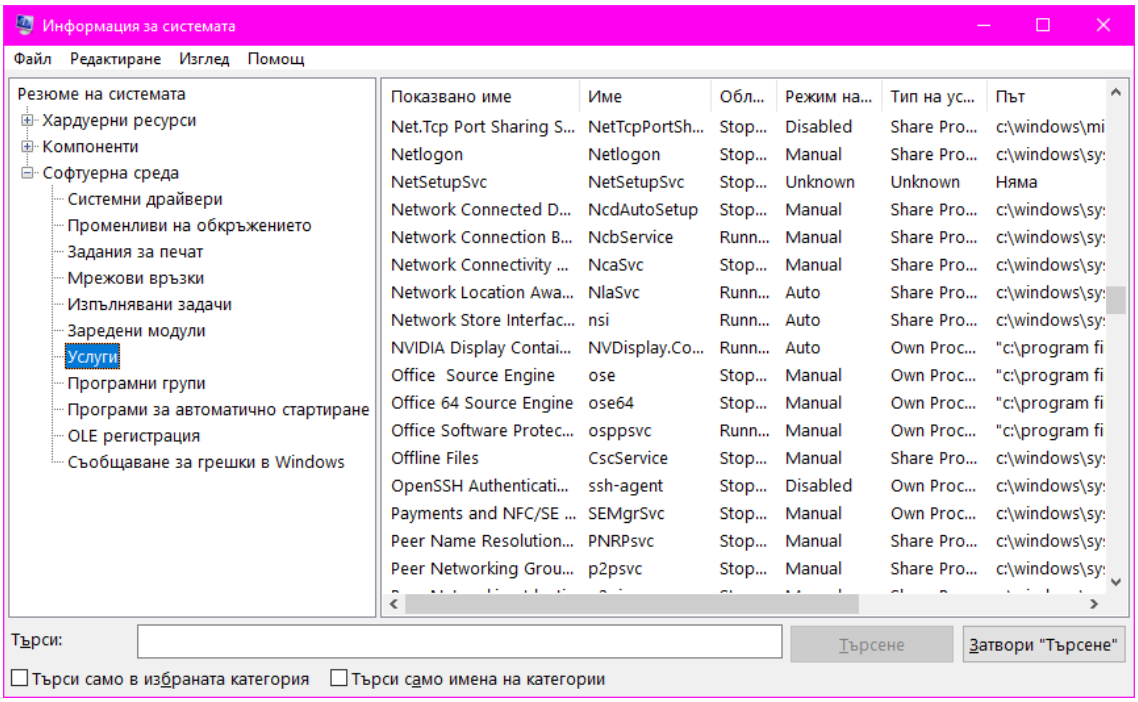
Разкриването на информация, относно съществуването на каквото и да е вредоносно програмно осигуряване, настроено за стартиране с Windows, може да стане в раздела на регистъра:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Обикновено когато там се появи вредоносна програма, тя създава услуга, поради което е задължително да се прегледа раздела:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`

Вредоносната услуга се търси по случайни имена и записи, които нямат сходство с профила на компютъра. По-удобен начин за преглеждане е чрез `msinfo32` (фиг. 6).



Фиг. 6: Информация за услугите

При правилна настройка на политиката за безопасност, всички услуги ще се показват според необходимостта. При разследвания в реално време, удобен инструмент за разследване на мрежова трасировка може да бъде Wireshark. При необходимост може да се използва `procdump`, който трябва да се инсталира, след свободно изтегляне от сайта на Microsoft.

Заключение

Решаването на проблемите, свързани със сигурността, изисква не само заучени ситуации, а трябва да се разчита и на натрупан опит. Специалистите са категорични, че всички стъпки при дадено разследване трябва да бъдат документирани, но при увереност, че натрупаните знания ще помогнат в последващи ситуации на злоумишлени събития. Направените изводи ще имат решаващо значение да недопускането на едни и същи грешки в бъдеще.

В много случаи за получаване на достъпа е откраднатa самоличност с повишени права, което представлява нарастваща заплаха. За целта трябва да се ограничи броя на потребителите с администраторски права, да се увеличи многофакторната автентификация, да се настроят допълнителни ограничения за влизане и т.н.

Синия отбор трябва да дава пълен отчет при документирането на изводи, както и напътствия за усъвършенстване на контрола по защитата на системата и мрежата.

Администраторите на мрежови системи, професионалистите по сигурността и мрежовите архитекти могат да получат подробна статистическа информация за прехвърлената информация между всички хостове и мрежови устройства в учреждението [2], [4].

References

1. Akbanov, M., Vassilakis, V., Logothetis, M. (2019). *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*. Journal of Telecommunications and Information Technology (JTIT) - 1/2019, ISSN 1509-4553, https://doi.org/10.26636/jtit.2019.130218.
2. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Educational simulation the local area network of academic departments with securely configured FTP server*. International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, pp. 146-154.
3. Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Routing information security in the local area network of academic departments using an enhanced distance vector routing protocol – EIGRP*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 35-46.
4. Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Security routing simulation the local area network of academic departments using a link-state routing protocol – OSPF*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 47-58.
5. Diogenes, Y., Ozkaya, E. (2018). *Cybersecurity – Attack and Defense Strategies*. Packt Publishing, ISBN 978-1-78847-529-7, Birmingham – Mumbai.
6. Diogenes, Y., Shinder, T. (2018). *Microsoft Azure Security Center*. Pearson Education, ISBN 978-1-5093-0703-6.
7. http://eddiejackson.net/azure/Azure_Security_Center_Documentation--MrNetTek.pdf
8. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf