Кибербезопасность

Владимир Яковенко / 22 ноября 2018 г.

Больше мощностей! Больше аналитики!

Видеокамеры – лёгкая и желанная мишень

- Разнообразие устройств, но однообразие компонент
- Как правило, слабая защита на программно-аппаратном уровне – понимание необходимости приходит не сразу
- Унификация дизайна – «фича» для одного может сыграть как «закладка» для другого
- Приоритет простоты и низкой стоимости монтажа и обслуживания над защитой от взлома
- Видеокамеры подключены 24/7 и по хорошим каналам, тренд на подключение и запись в облака
- Число установленных видеокамер взрывообразно растёт
- Никто ничего не проверяет, пока не грянет гром

Сегодняшние киберугрозы в среде IoT

30 млн устройств уже подключено

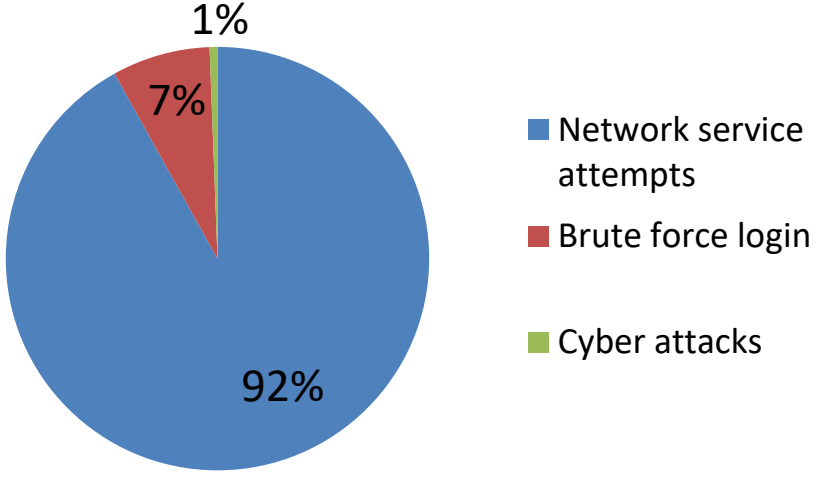
6 млрд пакетов данных анализируется ежедневно

1500 новых систем, совершающих хакерские атаки, обнаруживается ежечасно

Исследования в «реальном мире»

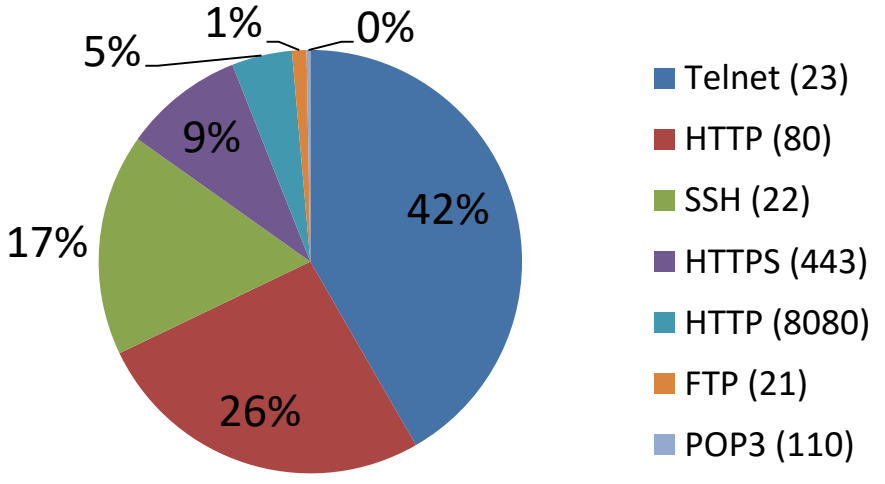
Период: 1-янв 2018 ~ 23-апр 2018 (4 месяца)
49 шт. IP видеокамер со спец. модулем на борту

Происшествия	Кол-во
Попытки подключения к сервисам	406,926
Подбор пароля	33,146
Кибератаки	2,640
Всего:	442,712



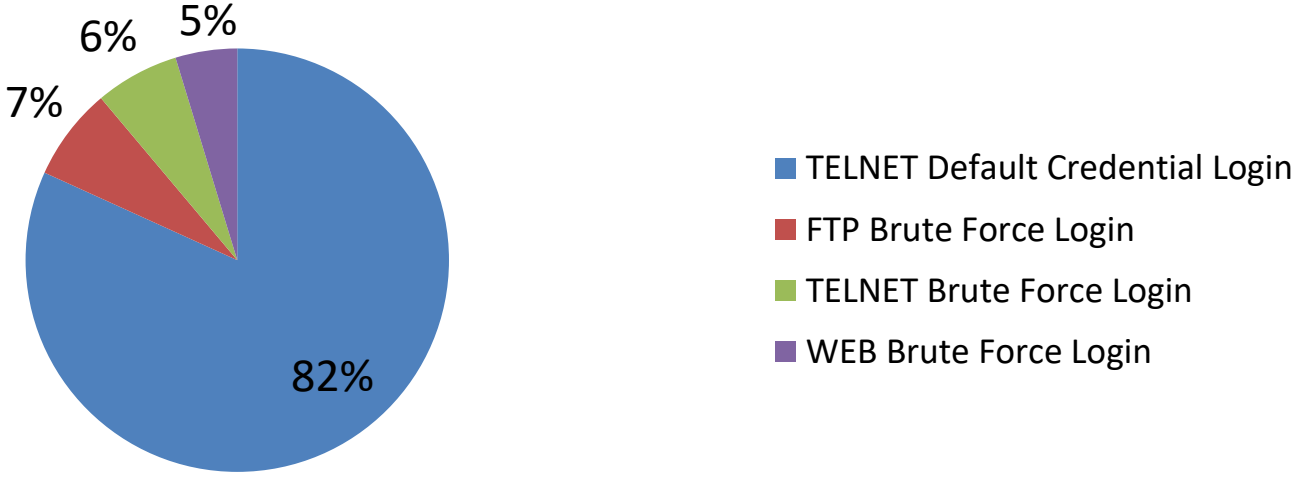
Попытки подключения к сервисам (92%)

Сервисы	Число попыток
Telnet (23)	169,620
HTTP (80)	106,587
SSH (22)	68,963
HTTPS (443)	37,336
HTTP (8080)	18,755
FTP (21)	4,522
POP3 (110)	1,143
Всего:	406,926



Грубый подбор пароля (7%)

Подбор пароля к сервисам	Число попыток
Пароль по умолчанию на TELNET	27,108
Пароль к FTP сервису	2,349
Пароль на TELNET	2,127
Пароль к WEB-интерфейсу	1,562
Всего:	33,146

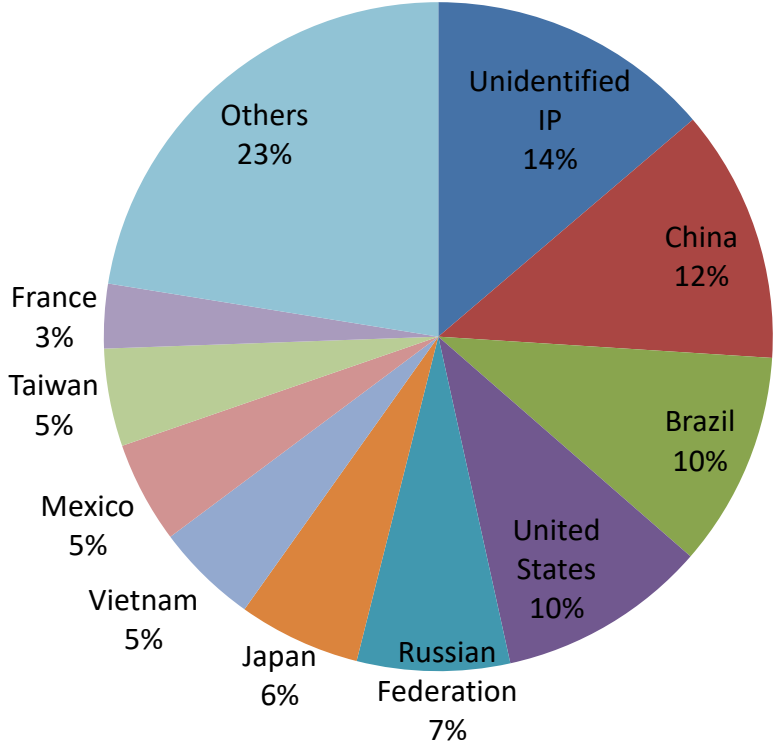


Кибератаки (1%)

Тип атаки (Top 10)	Число попыток
EXPLOIT Netcore Router default credential Remote Code Execution	874
EXPLOIT Netcore Router Backdoor Access	611
MALWARE Suspicious IoT Worm TELNET Activity -1	486
SHELLCODE Egg Hunter -1	133
WEB Apache Struts Dynamic Method Invocation Remote Code Execution -1.h	77
WEB GNU Bash Remote Code Execution -8.h (CVE-2014-6271;Shellshock)	59
WEB Remote File Inclusion /etc/passwd	49
MALWARE MIRAI TELNET Activity	43
EXPLOIT Remote Command Execution via Shell Script -2	39
RPC Novell NetWare NFS PortmapperRPC Module Stack overflow	37
Другие	1,106
Всего:	2,640

География источников атак

Страна	Кол-во
Неустановленные IP	60,938
Китай	54,217
Бразилия	46,013
США	44,886
Россия	32,693
Япония	26,165
Вьетнам	21,921
Мексика	21,785
Тайвань	20,894
Франция	13,772
Другие	99,428
Всего:	442,712



А много ли таких «дыр» в защите? – хватает

VIVOTEK

Historical List Of Exploits

This list contains a summary of known exploits in reverse chronological order. Additional details are provided in a section for each manufacturer below. Manufacturers with an asterisk (*) next to their name indicate products that were OEM'd under multiple brand names beyond the original manufacturer listed.

- July 2018 - Sony Talos 2018 Vulnerabilities - Allows commands to be executed without Admin credentials, however attacker needs to know what commands to execute so it is more complex than some other, simpler vulnerabilities.
- June 2018 - Axis VDOO 2018 Vulnerabilities - Results in root access, however the attack process is very complex, requires multiple steps and requires advanced linux knowledge and hacking skills.
- April 2018 - TBK (and OEMs) Vulnerability Provides Clear Text Credentials - a curl / http command provides the admin credentials of affected DVRs in plain text.
- April 2018 - Hikvision Critical Cloud Vulnerability - just knowing the registered email/phone number can get admin access. Note this was resolved before the date of disclosure.
- April 2018 - TVT Backdoor, Hardcoded authentication to download remote system configuration - including login and password in clear text
- January 2018 - Geovision 15 Backdoors and Vulnerabilities, including remote root access and clear text credentials
- December 2017 - Axis Vulnerabilities linked to DHCP and UPnP libraries in BisyBox, and vulnerability in CGI executables
- November 2017 - Hikvision Wifi cameras have hard-coded SSID, allows for rogue access point attack (7)
- November 2017 - Vivotek remote stack overflow vulnerability (3)
- November 2017 - Dahua Hard-coded backdoor credentials in camera and NVR firmware (6)
- October 2017 - Uniview recorders vulnerable to admin password retrieval backdoor
- August 2017 - Hikvision Tools allows admin password reset in older firmware (6)
- August 2017 - Hikvision iVMS-4200 stores passwords with reversible encryption (5)
- August 2017 - NeoCoolCam - iDoorbell product buffer overflow vulnerability allow various exp loits
- July 2017 - Dahua - Buffer overflow vulnerability in password field (5)
- July 2017 - Vivotek - CGI script exploits (2)
- July 2017 - Axis - Buffer overflow vulnerability in 3rd party software toolkit used for ONVIF (3)
- June 2017 - FLIR - Vulnerabilities allow remote code execution, unauthenticated viewing of live images, and reveal hard-coded accounts
- June 2017 - Persirai botnet attacks various consumer/SMB-oriented cameras.
- May 2017 - Hanwha - User can exploit cached data from a previous session to gain access to certain recorders
- March 2017 - Hikvision - Backdoor allows unauthorized access to admin interface (4)
- March 2017 - Axis - Multiple vulnerabilities related to CSRF attacks (2)
- March 2017 - Dahua - Backdoor allows attacker to read user/password list (4)
- March 2017 - Ubiquiti - Command injection vulnerability
- February 2017 - Geutebrück - Authentication bypass.
- February 2017 - Dahua - Multiple vulnerabilities in DHI-HCVR7216A-S3 recorders (3)
- December 2016 - Sony - Attackers can remotely enable telnet on cameras.
- December 2016 - Hikvision - hik-online.com servers susceptible to XXE exploit. (3)
- November 2016 - Milesight - Cameras have a number of vulnerabilities that allow remote exploit.
- November 2016 - Siemens - Remote privilege escalation possible via exploiting web interface.
- October 2016 - NUUO - Insecure default credentials. (2)
- October 2016 - Dahua*, XiongMai - Mirai botnet. (2)
- September 2016 - AVer - EH6108H+ DVR Multiple vulnerabilities
- August 2016 - NUUO - Remote root exploit and remote command injection vulnerability. (1)

Что делать? – Политика кибербезопасности

- Создание и ужесточение политик по обеспечению кибербезопасности продукции на всех этапах жизненного цикла продукции: разработка, тестирование, производство, поставка, монтаж, техобслуживание.

- Постоянное отслеживание ситуации и усиление всех видов деятельности в области обеспечения кибербезопасности.

- Регулярное обновление прошивок для производимых устройств с «заплатками» для всех обнаруженных проблем.

- Постоянное обучение и проведение «ликбезов» среди потребителей своей продукции.

- Выпуск руководства по усилению безопасности

Защита на этапе проектирования

- Ревизия как всей концепции работы оборудования так и собственно программного кода, с упором на:
  - Защиту от внедрения SQL кода
    Используются для атак на VMS или веб-порталы
  - Защиту от внедрения команд
    Ряд производителей видеокамер отличился недостаточной защитой
  - Переполнение буфера
    Используется хакерами в RTSP запросах для удалённого выполнения программного кода
- Валидация сертификатов SSL/TLS

Средства проверки на кибербезопасность

Работа со сторонними организациями - аудиторами

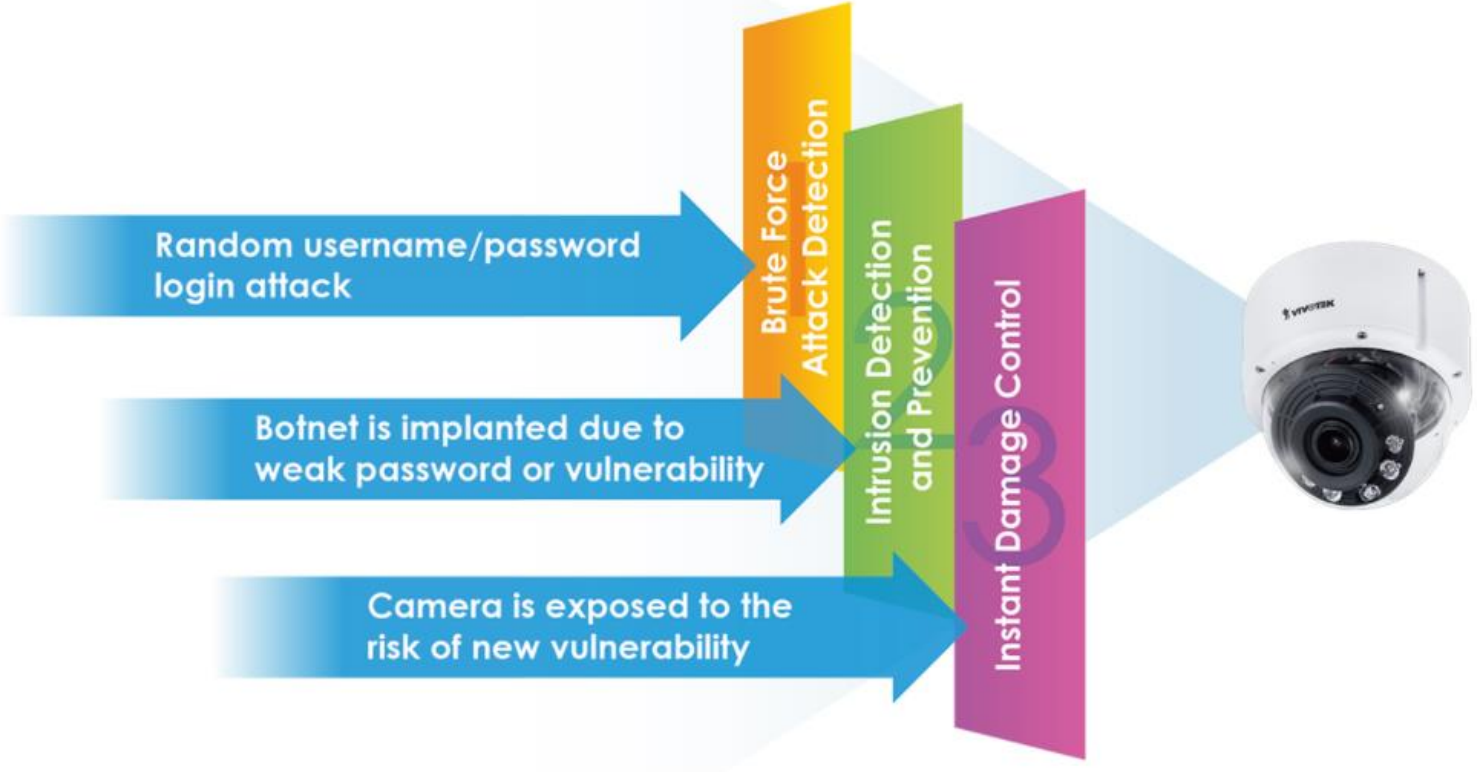
- Onward Security (https://www.onwardsecurity.com/)
  - Onward Security is a leader in developing technology that secures, defends, and responds to threats to information, distribution, and network systems on the connected things battlefield within both government and industrial sectors.

Работа со независимыми энтузиастами

- DEVCORE (https://devco.re/en/)
  - Offer penetration testing, consulting, training.
  - CEO: Allen Own (General Coordinator of Taiwan Hitcon)
  - Renowned hackers trying to crack products and find loopholes.

И наконец, старые добрые «антивирусы»

Уровни защиты для устройств систем видеонаблюдения



VIVOTEK

Благодарим за внимание, и приглашаем…

на Тайвань #безвиз